Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 191 (2021) 135–142

Procedia Computer Science

www.elsevier.com/locate/procedia

The 18th International Conference on Mobile Systems and Pervasive Computing (MobiSPC)
August 9-12, 2021, Leuven, Belgium

Federated Learning in Robotic and Autonomous Systems

Yu Xianjia[a,*], Jorge Peña Queralta[a], Jukka Heikkonen[a], Tomi Westerlund[a]

[a]*Turku Intelligent Embedded and Robotic Systems Lab, University of Turku, Turku, Finland*

Abstract

Autonomous systems are becoming inherently ubiquitous with the advancements of computing and communication solutions enabling low-latency offloading and real-time collaboration of distributed devices. Decentralized technologies with blockchain and distributed ledger technologies (DLTs) are playing a key role. At the same time, advances in deep learning (DL) have significantly raised the degree of autonomy and level of intelligence of robotic and autonomous systems. While these technological revolutions were taking place, raising concerns in terms of data security and end-user privacy has become an inescapable research consideration. Federated learning (FL) is a promising solution to privacy-preserving DL at the edge, with an inherently distributed nature by learning on isolated data islands and communicating only model updates. However, FL by itself does not provide the levels of security and robustness required by today's standards in distributed autonomous systems. This survey covers applications of FL to autonomous robots, analyzes the role of DLT and FL for these systems, and introduces the key background concepts and considerations in current research.

Keywords:
Robotics; Cloud Robotics; Fog Robotics; Federated Learning; Federated Reinforcement Learning; Federated Edge Learning; Distributed Learning; Distributed Ledger Technologies; Edge AI;

1. Introduction

With a staggering increase in the number of connected devices being deployed worldwide within the Internet of Things (IoT), the amount of data that is generated and transmitted has grown at exponential rates. The inefficiency of processing all this data in a centralized manner at the cloud has brought forward new computing and networking paradigms in recent years [1]. Computing at the edge nearby the data sources has evident benefits in terms of latency and bandwidth savings. Another key advantage is the inherent benefits to data privacy, as raw data does not travel too far. At the same time, the data is being fed to increasingly complex artificial intelligence (AI) models, with deep learning (DL) in particular becoming pervasive across multiple fields and application domains. Recent years have also

* Corresponding author.
E-mail address: xianjia.yu@utu.fi

1877-0509
10.1016/j.procs.2021.07.041

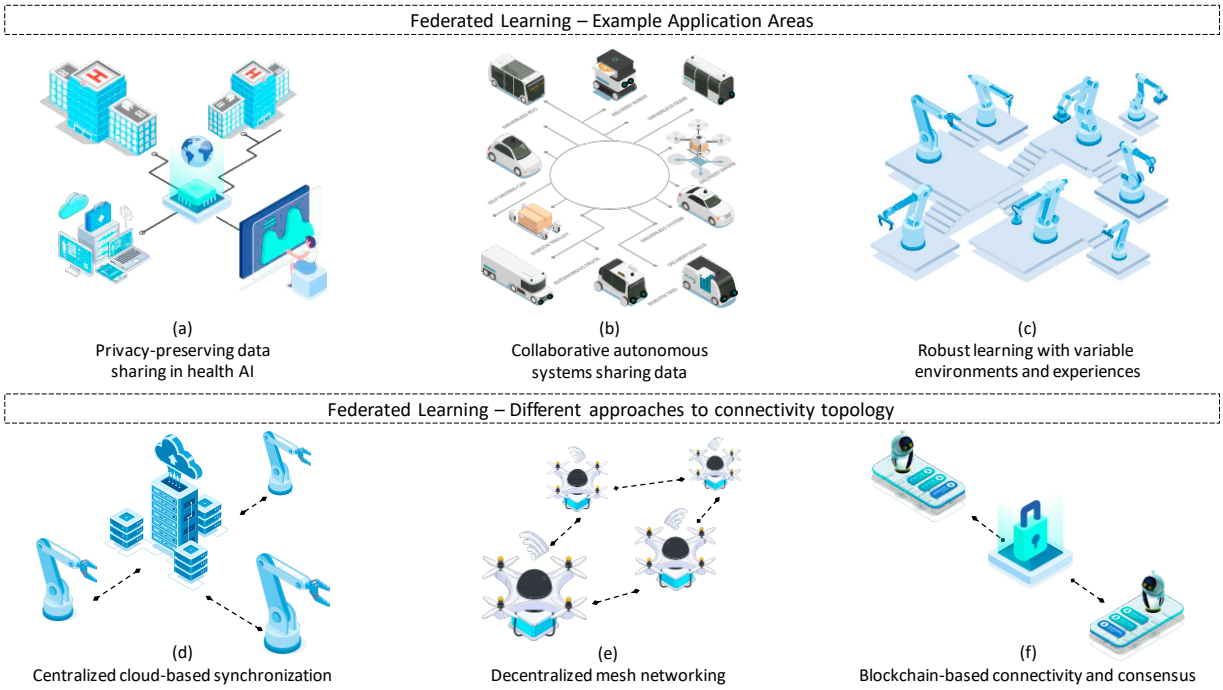

Fig. 1: Conceptual illustration showing potential application areas and connectivity topologies in federated learning systems.

brought an increasing awareness of the risks and drawbacks of sharing personal data over the internet. The solution to computing at the edge while preserving the privacy of data and leveraging DL solutions is federated learning [2]. Federated learning (FL) enables distributed training of complex models over isolated data islands from remote nodes (data sources). The local training results (updates to local models) are then aggregated, for example, in a cloud server, and a global generalized model is shared back to the nodes. All this with zero raw data transmission [3].

From the perspective of robotic and autonomous systems, which are becoming increasingly ubiquitous, cloud solutions have enabled higher degrees of intelligence by eliminating constraints of onboard computational and storage resources [4]. Cloud robotics and AI robotics are now an essential part of state-of-the-art robotic systems. Furthermore, as mobile connectivity evolves, 5G and beyond networks are set to further bring the integration of AI, robotics, and distributed networking solutions.Applications of AI in robotics include, e.g., the deployment of DL for natural language processing (NLP) [5], computer vision [6], or in navigation and mapping [7]. In control, Reinforcement learning (RL) has been successfully applied in complex games [8] and its relevance for dexterous manipulation extensively demonstrated [9]. Deep reinforcement learning (DRL) is particularly relevant to autonomous robots.

Multiple reviews and survey papers in the literature have been devoted to studying design approaches, implementation details, and application possibilities of FL. Compared to current works focused on security and privacy [10], personalized FL [11], or communication at the edge [12], the present work aims to provide a comprehensive view of how FL can be leveraged to raise the level of autonomy and degree of intelligence of robotic systems. We look at different application opportunities at the edge and within autonomous mobile robots. We provide an overview of the most important concepts and pay particular attention to synergies between FL and distributed ledger technologies (DLTs), among which blockchain technology has gained significant attention in recent years [13]. A conceptual illustration of FL applications and approaches to connectivity is shown in Figure 1.

2. Background

The adoption and development of FL frameworks have been directly or indirectly influenced by other technological and paradigm trends in robotics and autonomous systems. Since the invention of FL, there has been a lot of research carried out on the optimization of FL itself. Different research directions include increasing the adaptiveness, enhancing the privacy-preserving properties, or building towards more efficient collaboration for distributed robot learning,

among others. In this section, we briefly introduce the different identifiable research directions from the literature, and the concepts that underpin the popularity of FL in robotics and autonomous systems.

2.1. Cloud Robotics and Automation

Cloud robotics is a field of robotics that capitalizes on cloud technologies. The cloud infrastructure can provide robots and autonomous systems with extensive resources and potential benefits including big data, cloud computing, collective robot learning, and human learning [4]. Under cloud infrastructures, robotic systems have access to more collaborative approaches to autonomy, faster processing of deep learning models, and more powerful computational capabilities in general. A collection of robots in different areas or states can cooperate in a variety of tasks such as disaster management identifying several critical challenges [14] and manufacturing environment [15].

2.2. Distributed DL

With the increasing amount of data and complexity of DL models, the process of training models becomes inherently costly, computation-intensive, and time-consuming. Distributed DL was proposed to utilize the multiple processors to accelerate the DL training process by parallel the computation and the data [16, 17]. There is a significant amount of work in the literature dedicated to distributed DL in the pursuit of closer collaboration between cloud and edge computing [18, 19]. This balance between the two paradigms is set to become increasingly pervasive with a well-established IoT era. Immediate concerns that raise with the deployment of distributed DL across cloud and edge are the security of data and privacy of users. In consequence, multiple research directions have emerged to make distributed learning processes more scalable, secure, and privacy-preserving through [20, 21, 22]. Additionally, other research efforts are directed towards utilizing distributed DL for processing and learning from sensitive data such as health data [23] or medical data from multiple private or public institutions [24].

2.3. Privacy and Security In DL and FL

With the wider adoption of DL over the past decade, issues regarding data security and privacy of data sources became increasingly studied. Some of the main types of security-related issues in DL appear with evasion attacks during model inference and poisoning attacks during model training [25]. Adversarial attacks to the algorithms, and model reconstruction attacks are other examples. Multiple solutions have been proposed to deal with these and other attack vectors, including differential privacy, homomorphic encryption, data anonymization, pseudonymization, algorithm encryption, or hardware security implementations, among others [26]. Despite the efforts, new attack vectors have appeared such as re-identification attacks (identification of individual data sources despite data anonymization techniques based on other information in the datasets), dataset reconstruction attacks, or tracing attacks (also referred to as membership inference, though which the inclusion of a specific individual in a dataset is inferred). While FL itself offers privacy-preserving attributes, the security robustness depends largely on the implementation and deployment methodologies. A recent survey on the topic [10] presents a comprehensive study on the current security and privacy concerning aspects with the conclusion that fewer privacy-specific threats than security-specific ones exist. Among these are, e.g., communication bottlenecks, poisoning, and backdoor attacks, especially inference-based ones.

2.4. Federated and Distributed Reinforcement Learning

Multi-agent RL is regarded as essential to realize general intelligence and cooperative environment learning. The main objective of a multi-agent RL is to obtain the localized policies and maximize the global reward for knowledge sharing on the premise of increased system complexity and computation [27]. In multi-robot systems, distributed RL can be leveraged to expose different robots to different environments or to learn more robust policies in the presence of disturbances [28].

While the literature in distributed RL is extensive, most works rely on sharing raw experiences or training in a centralized manner. Federated RL (FRL) [29] has been proposed as an efficient solution for achieving high-quality policy transfer with the protection of both data and model privacy. FRL can be applied, e.g., to understand user behavior and adapt to it [30]. In [12], FRL was proposed to allow multiple RL agents to learn optimal control policies for a series of IoT devices with slightly different dynamics. In another direction, FRL is regarded as an efficient method for resource allocation among networked devices [31, 32].

2.5. Recent Developments of FL

Federated learning has arguably raised the possibilities for collaborative learning across multiple independent agents. In this section, we give an overview of works that have focused on improving specific aspects of FL.

With a focus on scalability, a high-level designed FL system based on TensorFlow has been developed that draws significant conclusions on existing challenges and future research directions [33]. From the perspective of system security, a systematic study of Byzantine-robust federated learning in [34] shows different approaches to secure FL systems and make them more robust against local model poisoning attacks. A similar approach in [35], instead considers a solution to detect the malicious model updates in every round of training process before aggregating the local models in the centralized cloud server. Owing to a wide range of approaches relying on a centralized cloud server for aggregation of local model updates, FL frameworks may fail if a malicious aggregation server takes over the central FL node. To cope with this problem, dispersed FL [36] has been proposed, where a global model is yielded in either a centralized or distributed manner through the aggregation of sub-global models, which are iteratively computed based on different groups similar to traditional FL approaches.

Machine learning itself can also play a role in improving the performance of FL systems. In [37], deep reinforcement learning is used to select the optimized edge nodes, and the learned model parameters are integrated into a blockchain-based FL scheme for enhanced security and reliability. Furthermore, combining with other privacy-preserving machine learning methods such as differential privacy [38] and modern cryptography techniques such as homomorphic encryption [39], FL can achieve high-level privacy-preserving and security capabilities.

It is also worth noting that FL solutions are specialized in aggregating local models to a global model for knowledge sharing. Nonetheless, in terms of the characterization of heterogeneous data collected across large-scale deployments of edge devices, it is often essential to the application to make the models discriminative in each device. In this direction, personalized FL was proposed to tackle the aforementioned problem by further performing a series of learning steps locally after receiving the global model from the cloud server, based mostly on locally available data for which the model needs to be tailored [40, 41].

3. Federated Learning at the Edge

Federated learning has emerged within the wider edge computing paradigm. Deploying FL at the edge has gained significant attention from the research community owing to the availability of rapidly increasing amounts of data and computational resources at the edge. Research directions include the deployment FL in resource-constrained embedded systems, communication-efficient FL, energy-efficient FL, and privacy-preserving federated edge learning with the aim to improve the learning performance in networks where the general assumption is that resources are inherently at the edge [42]. For instance, an early work explored how to capitalize on FL to optimize the caching scheme in the edge computing process [43].

3.1. Task Allocation

A general problem in distributed systems is task allocation. Learning more efficient task allocation at the edge can produce more effective strategies for worker selection and load distribution. Doing so through a distributed FL framework is a natural fit for such systems. In [44], a matching-theoretic approach was proposed for task assignments schemes in federated edge learning framework to solve the task assignment problem between the workers and multiple task publishers with efficient performance. In another work, an asynchronous task allocation method was introduced to realize equal task allocation within the FL system itself, i.e., minimizing the maximum difference between the number of model updates done by every worker in an FL edge network [45].

3.2. Communication and Energy Efficiency

Multiple studies in the literature focus on mitigating the bottleneck that communication latency can become in FL systems. Some of the proposed solutions involve the aggregation over the air of multiple updates from an analog perspective, rather than relying on conventional orthogonal network access [46]. In a similar direction, and to mitigate the communication overhead, authors in [47] introduced an asynchronous communication model for digital twin edge networks. In their work, FL is formulated as an optimization problem that aims at reducing the communication cost by

decomposing it and using DNN for communication resource allocation. In [48], compression techniques were utilized to realize a more communication-efficient FL solution.

Regarding the energy efficiency of FL, authors in [49] tackled the problem of improving the energy efficiency of FL by developing a convergence-guaranteed algorithm with flexible communication compression. In [50], two transmission protocols based on the non-orthogonal multiple access and time division multiple access were considered to jointly optimizing the transmission power and rate at edge devices in a federated edge learning system. Other authors showed that learning an optimal resource-management policy substantial energy can be reduced in an FL system [51].

3.3. Client Selection

Client selection is a process to choose model updates from certain clients to be aggregated, especially when computational resources are constrained and complex aggregation processes are not possible. In [52], a framework named FedCS (Federated Client Selection) was introduced to dynamically select and maximize the number of clients (training agents) in heterogeneous edge networks. The dynamic approach was based on an online estimation of actively available resources. The results show that such an approach can provide significantly better training performance with heterogeneity of resources across clients, with overall significantly shorter training times than traditional FL methods. In another work, an optimization algorithm is designed to jointly optimize the data sampling and user selection strategies, which is shown to approach the stationary optimal solution efficiently [53].

3.4. Privacy-Preserving and Secure Mechanism

While FL is flexible in nature and inherently deals with issues related to data ownership and governance, it does guarantee privacy and security by itself. Integration of other techniques and approaches to data security and user privacy needs to be considered to achieve a robust FL framework. For instance, an asynchronous FL system [54] with the incorporation of local differential privacy for enhanced privacy of local modes updates has been proposed in the literature [55]. To tackle the problem of active poisoning attacks, which FL is vulnerable to, authors in [56] generated a model for different poisoning attacks based on generative adversarial networks (GANs). Utilizing GANs, which is a well-established approach in DL research, opens the door to more robust FL systems.

4. Synergies between Federated Learning and Distributed Ledger Technologies

Distributed ledger technologies have multiple applications in multi-robot systems and distributed autonomous systems. Blockchain technology, in particular, has been applied to robot swarms able to deal with byzantine agents [57], for sharing computational and communication resources [58], but also for privacy-critical applications [59, 60]. The distributed consensus algorithms in DLTs, the auditability of operations, and the built-in encryption, among others, aid in designing more secure and privacy-preserving systems at the edge [13]. Blockchain technology and subsequent DLT solutions can be thus leveraged as the basis for trust and credibility in a distributed system.

Traditional FL approaches rely on a centralized cloud server for model aggregation, therefore assuming such a central node has full trust from the rest of the system. In practice, the reliance on the cloud server and the transmission to the local clients can be threatened by various types of malicious attacks. Additionally, the scalability of the system is inherently limited by the existence of a single processing node. Even if it is replicated in the cloud, there is still a strong reliance on trusted cloud servers. Therefore, being able to deploy trustable FL frameworks in a distributed and decentralized manner can take FL to new application domains [61, 62, 63].

The literature on applications of DLTs and FL for robotic systems is sparse. At present, studies on applications of blockchain-enhanced FL mainly focus on autonomous vehicles and the Internet of Vehicles (IoVs). The core objective of these studies is to build a trustworthy vehicular network without any centralized training process or trusted third party. In this direction, blockchain-supported FL has been proposed to build a trustworthy vehicular network. with performance metrics including accuracy, energy consumption, and lifetime rate, along with throughput and latency evaluated by simulation [64]. It is worth mentioning as well that a hierarchical blockchain-based FL has also proved to be efficient in building towards large-scale vehicular networks and shown potential resilience against certain malicious attacks [65]. In another work, an autonomous blockchain-enabled FL has been proposed to add further privacy-preserving properties and efficient local on-vehicle machine learning model aggregation in a decentralized manner [66]. The authors indicate some key challenges of the proposed framework in the autonomous vehicles field including sophisticated mobility models, mobility-aware and efficient verification, or privacy leakage risk analysis.

Other examples of blockchain-enhanced FL include drones in 6G networks and control in railway systems. In [67], the objective is to replace the manual fraction and braking operations with automatic operations in a heavy haul railway system. They utilized blockchain-based FL to obtain a novel ML model for intelligent control under the circumstance of the imbalanced fraction and braking data. One approach to build the foundations for the upcoming 6G era, a blockchain-based empowered FL with the applications of mobile miners at drones has been proposed for a disaster response system [68]. In this work, the authors mainly focused on the definition of frameworks and analysis of blockchain latency and energy consumption.

5. Applications of FL In Robotic and Autonomous System

Networked robotic and autonomous systems are becoming ubiquitous. These agents are in turn increasingly heterogeneous in terms of their computational capabilities but also the type of data they produce. With the wider availability of unprecedented amounts of data, deep learning has been broadly employed across autonomous robots of all types. Cloud robotics unlocks for robotic and autonomous systems access to potentially unlimited computational, memory or storage resources, partially avoiding the limitations of onboard resources. Cloud robotics also offers the use of the internet for massive parallel computing and resource sharing [69]. At the same time, autonomous robotic solutions have been adopted across a growing number of industries and application domains. These include data-sensitive scenarios such as hospitals, military bases, or hotels. On account of features ranging from privacy preservation, decentralized reliability, minimal communication and focus on onboard computation, it is arguable that federated learning has the potential to be a secure and efficient robot learning framework in and it will be further adopted across different types of autonomous systems [70].

From a system-level perspective, different nomenclatures are used to define the paradigm of shared computation across and between cloud and edge. In this area, fog robotics has been introduced as the paradigm of deploying robot deep learning across shared computational, storage, and networking resources between cloud and edge in a federated way. In [71], the authors evaluated the performance of the designed fog robotics system through a surface decluttering application with object recognition approaches. They trained the deep models in the cloud server based on the non-private images, adapted and deployed the model based on the real-world images on the edge side to reduce the round-trip communication cost. In another application of fog robotics, blockchain-based FL has been proposed for autonomous vehicles which enables a communication network where on-vehicle machine learning models are verified and exchanged in a distributed and privacy-aware fashion [68]. The authors evaluate the performance of generation delay, block propagation, and upload-download delay, showing promising applications of such frameworks.

Federated learning has potential within multiple specific autonomy problems and robotic subsystems. In [72], cooperative SLAM based on visual-Lidar has been proposed by deploying a federated deep learning algorithm for feature extraction and dynamic map fusion without transferring original images among the robots. In the area of dynamic map fusion, authors in [73] developed a novel fusion scheme among the networked vehicles supported by FL. Superior performance and robustness were then demonstrated in the Car Learning to Act (CARLA) simulation platform. In [74], trajectories forecasting (Spatio-temporal predictions) has been performed in a multi-robot system through different FL variants: traditional FL approach where a cloud server aggregates the local models and serverless version. In the paper, the authors found that in a trajectories forecasting task, the results of the above methods are not notably different and they provided the first federated learning dataset obtained from multi-robot behaviors. FL has also proven to be an efficient and novel framework in heterogeneous sensor data fusion for imitation learning [75]. In terms of situational awareness, continuous learning has been demonstrated to be feasible through FL as a framework across computationally limited edge devices while enabling the post-deployment of learned models in inference-only mode [76]. In [12], FRL was applied to learn an optimal control policy among multiple IoT autonomous devices of the same type. In [77], the authors introduced an FL-based online reinforcement transfer learning process for real-time perception, with a demonstration through a collision-avoidance system simulated in Airsim. From a more general autonomous navigation perspective, planning modules in cloud robotic systems can utilize federated reinforcement learning as a learning architecture for fusing prior knowledge and quickly adapting to new environments [7].

In the area of human-robot collaborative learning, a novel cognitive architecture based on FL was introduced for multi-agent learning from demonstration (LfD) with multiple humans incorporated in the self robot learning loop [78]. In a subsequent study, the authors integrated the short- and long-term analysis of human behavior within their cognitive robot learning architecture to show that it can adaptively enhance large-scale multi-agent LfD [79].

6. Conclusion

FL offers advantageous solutions to collaborative learning in decentralized multi-robot systems and distributed autonomous systems. FL will play a key role in networked ubiquitous robots and autonomous intelligent systems at the edge. The vast and rapidly growing amount of research in the area is revealing the efficiency and applicability of FL in various solutions.The key advantages of FL solutions include the optimization of networking resources, resilience through decentralization, and inherent privacy-preserving properties by processing data directly at the edge.

We also reviewed DLT-empowered FL with DLTs that has drawn significant attention in the robotics domain in recent years. DLT solutions, and blockchain technology, in particular, can be the backbone of decentralized local model aggregation in a more privacy-preserving, secure, and distributed manner. Some of the most prominent results are being shown in the era of the internet of vehicles, set to become increasingly important with the wider adoption of 5G and beyond mobile connectivity solutions.

In summary, FL has multiple application possibilities in autonomous systems either from a system-level perspective or within specific subsystems like in autonomous robots. Key research directions that need further exploration include optimization of communication, energy efficiency at the edge, personalized FL, and further privacy and security enhancements. Research efforts are currently capitalizing on multidisciplinary approaches including modern encryption, novel connectivity topologies, or new learning paradigms.

Acknowledgements

This research work is supported by the Academy of Finland's AutoSOS project (Grant No. 328755) and RoboMesh project (Grant No. 336061).

References

[1] W. Shi et al., Edge computing: Vision and challenges, IEEE IoT Journal (2016).
[2] Q. Yang et al., Federated machine learning: Concept and applications, ACM TIST (2019).
[3] Y. Liu et al., Federated learning for 6g communications: Challenges, methods, and future directions, China Communications (2020).
[4] B. Kehoe et al., A survey of research on cloud robotics and automation, IEEE Transactions on automation science and engineering (2015).
[5] C. Matuszek et al., Grounded language learning: Where robotics and nlp meet (invited talk), in: IJCAI, 2018.
[6] J. Ruiz-del-Solar et al., A survey on deep learning methods for robot vision, arxiv:1803.10862 (2018).
[7] B. Liu et al., Lifelong federated reinforcement learning: a learning architecture for navigation in cloud robotic systems, RA-L (2019).
[8] K. Shao et al., A survey of deep reinforcement learning in video games, arxiv:1912.10944 (2019).
[9] P. Henderson et al., Deep reinforcement learning that matters, in: AAAI Conference on Artificial Intelligence, 2018.
[10] V. Mothukuri et al., A survey on security and privacy of federated learning, Future Generation Computer Systems (2021).
[11] V. Kulkarni et al., Survey of personalization techniques for federated learning, in: WorldS4, IEEE, 2020.
[12] W. L. et al., Federated learning in mobile edge networks: A comprehensive survey.
[13] J. P. Queralta et al., Blockchain for mobile edge computing: Consensus mechanisms and scalability, arxiv:2006.07578 (2020).
[14] W. Chen et al., A study of robotic cooperation in cloud robotics: Architecture and challenges, IEEE Access 6 (2018) 36662–36682.
[15] H. Yan et al., Cloud robotics in smart manufacturing environments: Challenges and countermeasures, Comp. & Electrical Eng. (2017).
[16] E.P. Xing et al., Petuum: A new platform for distributed machine learning on big data, IEEE Transactions on Big Data (2015).
[17] Z. Tang et al., Communication-efficient distributed deep learning: A comprehensive survey, arxiv:2003.06307 (2020).
[18] H. Wu et al., Collaborate edge and cloud computing with distributed deep learning for smart city internet of things, IEEE IoT Journal (2020).
[19] H. Jiang et al., Distributed deep learning optimized system over the cloud and smart phone devices, IEEE Trans. on Mobile Computing (2019).
[20] S. Shi et al., Towards scalable distributed training of deep learning on public cloud clusters, Machine Learning and Systems (2021).
[21] Y. Li et al., Toward secure and privacy-preserving distributed deep learning in fog-cloud computing, IEEE IoT Journal (2020).
[22] D. Buniatyan, Hyper: Distributed cloud processing for large-scale deep learning tasks, in: CSIT, IEEE, 2019.
[23] P. Vepakomma et al., Reducing leakage in distributed deep learning for sensitive health data, arxiv:1812.00564 (2019).
[24] N. Balachandar et al., Accounting for data variability in multi-institutional distributed deep learning for medical imaging, JAMIA (2020).
[25] H. Bae et al., Security and privacy issues in deep learning, arxiv:1807.11655 (2018).
[26] G. A. Kaissis, M. R. Makowski, D. Rückert, R. F. Braren, Secure, privacy-preserving and federated machine learning in medical imaging, Nature Machine Intelligence 2 (6) (2020) 305–311.
[27] W. Zhao et al., Sim-to-real transfer in deep reinforcement learning for robotics: a survey, in: IEEE SSCI, IEEE, 2020.
[28] W. Zhao et al., Towards closing the sim-to-real gap in collaborative multi-robot deep reinforcement learning, in: 5th ICRAE, IEEE, 2020.
[29] H. H. Zhuo et al., Federated reinforcement learning, arxiv:1901.08277 (2019).
[30] C. Nadiger et al., Federated reinforcement learning for fast personalization, in: IEEE 2nd AIKE, IEEE, 2019.

[31] L. Ruan et al., Low-latency federated reinforcement learning-based resource allocation in converged access networks, in: Optical Fiber Communication Conference, Optical Society of America, 2020.
[32] H.T. Nguyen et al., Resource allocation in mobility-aware federated learning networks: a deep reinforcement learning approach, in: WF-IoT, IEEE, 2020.
[33] K. Bonawitz et al., Towards federated learning at scale: System design, arxiv:1902.01046 (2019).
[34] M. Fang et al., Local model poisoning attacks to byzantine-robust federated learning, in: 29th {USENIX} Security Symposium ({USENIX} Security 20), 2020.
[35] S. Li et al., Learning to detect malicious clients for robust federated learning, arxiv:2002.00211 (2020).
[36] L. U. Khan et al., Dispersed federated learning: Vision, taxonomy, and future directions, arxiv:2008.05189 (2020).
[37] Y. Lu et al., Blockchain empowered asynchronous federated learning for secure data sharing in internet of vehicles, IEEE Transactions on Vehicular Technology (2020).
[38] K. Wei et al., Federated learning with differential privacy: Algorithms and performance analysis, IEEE Trans. Inf. Forensics Secur. (2020).
[39] C. Zhang et al., Batchcrypt: Efficient homomorphic encryption for cross-silo federated learning, in: {USENIX}, 2020.
[40] Y. Deng et al., Adaptive personalized federated learning, arxiv:2003.13461 (2020).
[41] A. Fallah et al., Personalized federated learning: A meta-learning approach, arxiv:2002.07948 (2020).
[42] S. Wang et al., Adaptive federated learning in resource constrained edge computing systems, IEEE J. Sel. Areas Commun. (2019).
[43] Z. Yu et al., Federated learning based proactive content caching in edge computing, in: IEEE GLOBECOM, IEEE, 2018.
[44] J. Kang et al., Training task allocation in federated edge learning: A matching-theoretic approach, in: IEEE 17th CCNC, IEEE, 2020.
[45] U. Mohammad et al., Adaptive task allocation for asynchronous federated mobile edge learning, arxiv:1905.01656 (2019).
[46] G. Zhu et al., Broadband analog aggregation for low-latency federated edge learning (extended version), arXiv:1812.11494 (2018).
[47] Y. Lu et al., Communication-efficient federated learning for digital twin edge networks in industrial iot, IEEE Trans Industr Inform (2020).
[48] J. Mills et al., Communication-efficient federated learning for wireless edge intelligence in iot, IEEE IoT Journal (2019).
[49] L. Li et al., To talk or to work: Flexible communication compression for energy efficient federated learning over heterogeneous mobile edge devices, arxiv:2012.11804 (2020).
[50] X. Mo et al., Energy-efficient federated edge learning with joint communication and computation design, arXiv:2003.00199 (2020).
[51] Q. Zeng et al., Energy-efficient radio resource allocation for federated edge learning, in: IEEE ICC Workshops, IEEE, 2020.
[52] T. Nishio et al., Client selection for federated learning with heterogeneous resources in mobile edge, in: IEEE ICC, IEEE, 2019.
[53] C. Feng et al., Joint optimization of data sampling and user selection for federated learning in the mobile edge computing systems, in: IEEE ICC Workshops, IEEE, 2020.
[54] X. L. et al., Privacy-preserving asynchronous federated learning mechanism for edge network computing.
[55] Y. L. et al., Differentially private asynchronous federated learning for mobile edge computing in urban informatics.
[56] J. Z. et al., Poisongan: Generative poisoning attacks against federated learning in edge computing systems.
[57] E. C. Ferrer, The blockchain: a new framework for robotic swarm systems, in: Future technologies conference, Springer, 2018.
[58] J. P. Queralta et al., Blockchain-powered collaboration in heterogeneous swarms of robots, arxiv:1912.01711 (2019).
[59] A. Nawaz et al., Edge ai and blockchain for privacy-critical and data-sensitive applications, in: ICMU, IEEE, 2019.
[60] A. Nawaz et al., Edge computing to secure iot data ownership and trade with the ethereum blockchain (2020).
[61] D. C. Nguyen et al., Federated learning meets blockchain in edge computing: Opportunities and challenges, arXiv:2104.01776 (2021).
[62] X. Bao et al., Flchain: A blockchain for auditable federated learning with trust and incentive, in: 5th BIGCOM, IEEE, 2019.
[63] U. Majeed et al., Flchain: Federated learning via mec-enabled blockchain network, in: 20th APNOMS, IEEE, 2019.
[64] S. Otoum et al., Blockchain-supported federated learning for trustworthy vehicular networks, in: GLOBECOM, IEEE, 2020.
[65] H. Chai et al., A hierarchical blockchain-enabled federated learning algorithm for knowledge sharing in internet of vehicles, IEEE Transactions on Intelligent Transportation Systems (2020).
[66] S. R. Pokhrel et al., Federated learning with blockchain for autonomous vehicles: Analysis and design.
[67] H. Gaofeng et al., Blockchain-based federated learning for intelligent control in heavy haul railway (2020).
[68] S. R. Pokhre , Federated learning meets blockchain at 6g edge: A drone-assisted networking for disaster response, in: ACM MobiCom Workshop on Drone Assisted Wireless Communications for 5G and Beyond, 2020.
[69] K. Goldberg et al., Cloud robotics and automation: A survey of related work, EECS Department, University of California, Berkeley, Tech. Rep. UCB/EECS-2013-5 (2013).
[70] S. Savazzi et al., Opportunities of federated learning in connected, cooperative and automated industrial systems, arxiv:2101.03367 (2021).
[71] A. K. Tanwani et al., A fog robotics approach to deep robot learning: Application to object recognition and grasp planning in surface decluttering, in: IEEE ICRA, IEEE, 2019.
[72] Z. Li et al., Fc-slam: Federated learning enhanced distributed visual-lidar slam in cloud robotic system, in: IEEE ROBIO, IEEE, 2019.
[73] Z. Zhang et al., Distributed dynamic map fusion via federated learning for intelligent networked vehicles, arxiv:2103.03786 (2021).
[74] N. Majcherczyk et al., Flow-fl: Data-driven federated learning for spatio-temporal predictions in multi-robot systems, arxiv:2010.08595 (2020).
[75] B. Liu et al., Federated imitation learning: A novel framework for cloud robotic systems with heterogeneous sensor data, RA-L (2020).
[76] Busart III et al., Federated learning architecture to enable continuous learning at the tactical edge for situational awareness, Ph.D. thesis, The George Washington University (2020).
[77] X. Liang et al., Federated transfer reinforcement learning for autonomous driving, arxiv:1910.06001 (2019).
[78] G.T. Papadopoulos et al., Towards open and expandable cognitive ai architectures for large-scale multi-agent human-robot collaborative learning, arxiv:2012.08174 (2020).
[79] G.T. Papadopoulos et al., User profile-driven large-scale multi-agent learning from demonstration in federated human-robot collaborative environments, arxiv:2103.16434 (2021).