# The State of Federated Learning in Robotics and Autonomous Systems: Past, Present and Future

Rishita Mavani[1], Aayushi Lad[1], Abhay Parmar[1], Keval Patani[1], Jay Patel[1], and Prof. Himani Trivedi[1]

[1]Computer Engineering Department, LDRP Institute of Technology and Research, Gandhinagar, Gujarat, India

**February 2023**

## 1 Abstract

To overcome the challenges of data sensibility and data silos the federated learning (FL) is used. It is a collaboratively decentralized privacy-preserving technology. Over the decade, deep learning has shown significant progress in robotics and autonomous system. This raised the concern in the matter of data security and privacy. In federated learning, the data is decentralized and the model moves towards the data, thus, the training happens with end devices. Federated Learning (FL) has the potential to protect privacy in Deep Learning (DL) at the edge. It achieves this by working in a decentralized manner, where it learns from separate data sources and exchanges only the model updates, thus maintaining the isolation of data islands. This survey paper covers the study of federated learning in robotics and autonomous system, introducing the current work in the field and its future scope of it.

## 2 Introduction

With increase in the number of connected devices and data deployed worldwide. And use of artificial intelligence techniques such as machine learning and deep learning to process data generated from end devices to increase the user experiences or to crate beater model. It becomes harder to process all those data and also maintain the security of end user data. Requiring more Complex system and security measurement thus increasing the time to process those data and make it even harder to maintain it and also it become harder to gather all the data from end user and process them to train in centralized method. To make it easy to maintain the security and make it easier to processing end user data We can use Federated Learning.

Technically, Federated Learning is a distributed collaborative AI approach that allows for data training by coordinating multiple devices with a central server without sharing actual datasets [7].In federated learning the global model is trained with local data then the train model is downloaded by the client user which are capable of running the model then the model is trained in client user device and then the global request the parameters of clients model and combine them all to construct new improved model.

By training model locally and using user data in their local devices to train model it element the process of sending user personal data to the centralized server thus increasing the security of user data and it's also make it easier to train model because the user data is processed locally and then important parameters are fetched from them thus it require less processing power to process or to train the next model and make the process more easier and faster. Let's discuss some of the use of Federated Learning in real word.

Federated Learning can be used to train robots in warehouses to tack the shortest path and farther make it more intelligent to train other robot. each robot continually collects the data and train them self from its local data and by sharing the model data with another robot to train that model too. It also makes it easier to add new robots in the warehouse because the new robot can gather the model-related data from already running robots and can run without interfering with the other robot's path.[10]

Federated Learning can be used in Autonomous vehicles. Each vehicle on the road can gather really vast amounts of data to train to model and can be trained using their own data and then share the model to the less use of droved vehicles and can also be used to train global models to implead in new model and cars. making it easier to train Autonomous vehicles and decrease the number of accidents of vehicles.[6]

# 3 Related Work

## 3.1 History of Federated Learning

Google first discussed the term 'Federated Learning' in a paper published in 2016 until then models were trained using centralized data. Also, 2016 is the year when Artificial Intelligence(AI) was fully established. Many of these AI applications were trained using a centralized approach which had the benefit of keeping models and data at one centralized location which was very easy to handle. Still, this approach had many downsides like issues with connectivity and many more unpredictable issues and today's AI is shifting towards Decentralized Learning. Since then this topic has been an active research area [18]. During this time use and misuse of personal data were happening globally. Facebook and other application Users were awakened about the dangers of shar-

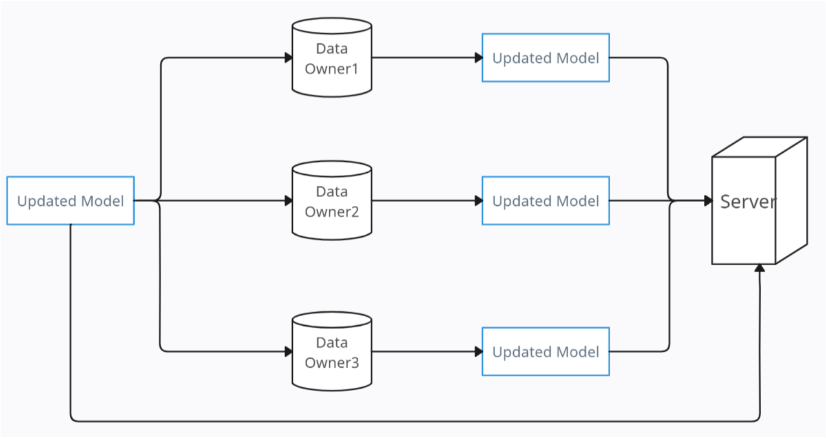

Figure 1: Architecture of Federated Learning

ing personal information online. Different research directions include increasing adaptiveness, enhancing privacy-preserving properties, or building towards more efficient collaboration for distributed robot learning, among others.[17]

In a decentralized Multi-Robotic system Federated Learning has always given much better results than any other centralized system. In networked ubiquitous robots and autonomous intelligent systems, Federated Learning will play a key role[17]. Federated Learning has given a boost to a decentralized system that not only gives good security to user data but also gives a secure and faster way to train any model. Key reasons for using Federated Learning are, Networking Resources have been optimized and privacy-preserving properties can be directly inherited at the edge[17].

## 3.2 Evolution of Federated Learning

Networked robotic and autonomous systems are becoming ubiquitous[17]. The primitive framework of FL is FedAvg. Though it could deal with some lightweight Non-IID data.[8] Recent work focuses on optimizing algorithms to improve efficiency and protect users' data.

Federated Learning has raised opportunities for collaborative learning between multiple independent platforms.[17] As scalability was the main focus a high-level Federated Learning system was developed based on TensorFlow.[17] From the perspective of system security, a systematic study of Byzantine-robust federated learning in[3] shows different approaches to secure FL systems and make them more robust against local model poisoning attacks. It still faces challenges with structural heterogeneity and high communication overhead.[8]

Over the years Distributed approach to learning has been developed widely. Federated Learning was developed with the goal of training a high-level centralized model while the training data stays distributed on different devices and other connected devices training data does not get affected.[4] Now every different device can train the model individually with their own personal training data without affecting other devices and can easily make changes in central data after training the model.[4]

In 2019, [18] extended the original 'federated learning' to a general concept for all privacy-preserving decentralized collaborative machine learning techniques. The paper briefly describes types of Federated Learning that are Horizontal FL and Vertical FL.

In 2020, [8] published a paper that describes the current progress of FL in fields like the Internet Of Things(IoT), Healthcare, driven cars, and debit card fraud efficiency[8]. It discusses how Federated Learning has changed the perspective of these fields.

### 3.3 Other Use-Cases

Federated Learning has numerous use cases in each and every field of work. Federated Learning has shown astonishing results in identifying cancer patients with its large, diverse, and uncentralized data which helps in providing life-saving treatment to the needy. A consumer always needs the security of its data which is cleverly handled through federated learning. Federated learning keeps the data safe and intact without affecting the training of the model and so it is more reliable. In a centralized system, the fraud rates were increasing rapidly which lead to financial crises that have been now reduced due to federated learning. In the old centralized system, there were trust issues between different co-workers working on the same model about making changes in their work but now everyone can update the model with their data without affecting others' models and data. Federated learning keeps the original data safe and changes are affected at the user end only by this we can preserve the original data and can regain it anytime when needed.

## 4 Overview

### 4.1 Categorization of FL

FL largely falls into three groups, respectively, horizontal FL, vertical FL, and federated transfer learning. Since data stored in different nodes or institutions mainly exist in a feature matrix form.

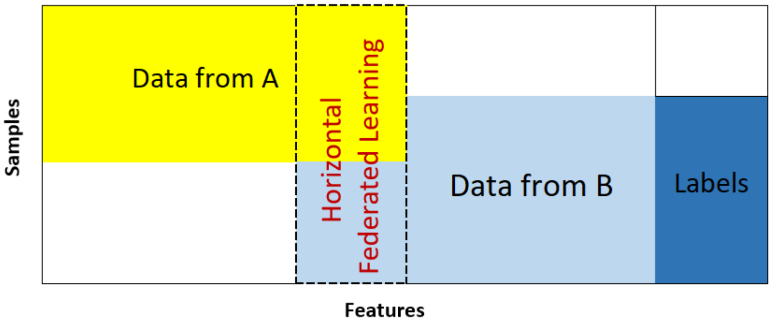

Figure 2: Horizontal Federated Learning

### 4.1.1 Horizontal FL

In the case of horizontal FL, there is a some amount of overlap between the feature of data spread across various nodes, while the data are quite different in sample space not in feature space. The FL algorithms are primarily aimed at applications in smart devices or devices in the internet of things. FL in these scenarios usually could be classified into horizontal FL, Because data may significantly different in sample space but have similar feature space. [8] In case of HFL systems, all learning clients cooperatively train a global FL model using their local datasets with the same feature space but different sample space. In this, each client locally trains its AI model to compute a local update. For improved security, the computed local update can be masked by using encryption or differential privacy techniques, but usally the encryption technique. Then, the server aggregates all local updates from clients and computes the new global update without the need for direct access to local data. Horizontal federated learning is follow the scenarios in which datasets on the participating clients share the different samples but have the same feature space.[20] Finally, the server sends back the global update to all clients for the next round of local learning. And The above process iterates until the loss function converges or a desirable accuracy is achieved. In Internet Of Things applications, an example of HFL is Wake-word detection, e.g., voice assistants in a smart home and etc. In this case, users speak the same sentence (feature space) with the different types of voice (sample space) on their smartphones and then the local speaking updates are parameter server to create a global model for voice recognition.[13]

### 4.1.2 Vertical FL

VFL solves the shared AI model learning in a network of clients which have the same sample space with different data feature spaces, this is how the VFL diffenet from HFL. Vertical federated learning is similar to feature distributed learning to some extent which 'vertically' partitions portion the training data, upon the feature space.[20] An entity alignment approach is adopted to collect the overlapped data samples of clients. These samples are combined to train a common AI model using encryption techniques or differe privacy technique. For an example in IoT applications can be the shared learning model among entities in a smart city, e.g.,banking institution and ecommerce companies. In smart city, an e -commerce company and a bank (different data feature) which serve city customers (same sample space) can join a VFL process to cooperatively train an AI model using their datasets. For an example, historic user payment at e-commerce companies and user account balance at the bank.By using this model, VFL can estimate the optimal personalized loans for all customers based on their online shopping behaviours.[13]. By the reports or survey Vertical FL is suitable for cases in which data is partitioned in the vertical direction according to feature dimension. [8]

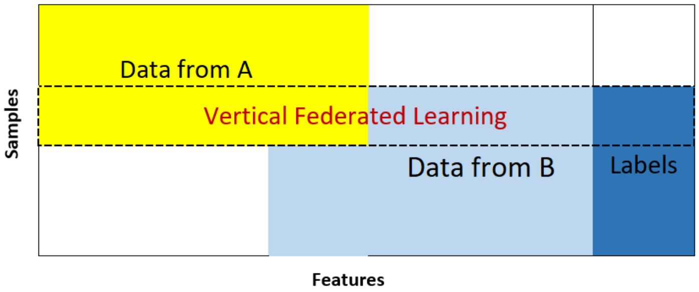

Figure 3: Vertical Federated Learning

#### 4.1.3 Federated transfer learning

Federated transfer learning applies to the scenarios in which two datasets different not only in samples but also in feature space. Let Consider two institutions: one is a bank located in China and the other one is an e-commerce company located in the United States (we can choose others also).As per geographical restrictions, the user groups of the two institutions have a small intersection. On the other side, owing to the different businesses, only a small portion of the feature space from both parties overlaps. In this case, transfer-learning techniques can be applied to provide solutions for the entire sample and feature space under a federation it is how the FTL used.In this Specially, A common representation between the two feature spaces is learned using limited common sample sets and later applied to obtain predictions for samples with only one-side features.[18] The aim of FTL is to extend the sample space from the VFL architecture with more learning clients that have datasets with different sample spaces and different feature spaces. Due to the differences in the nature of business, such enterprises share only a small overlaped in feature space. This is also applicable to the enterprises set up far in Ground. But in such scenarios, datasets differ both in samples and in feature space. Transfer learning technique aim to build effective model for the target domain while leveraging knowledge from the other source or domains.[14] FTL transfers feature from different feature spaces to the same representation that is used to train data aggregated from multiple clients or sources. Also, to preserve data privacy and ensure security in FTL, encryption techniques such as random masks are also employed to encrypt gradient updates in the model update stage.[13]

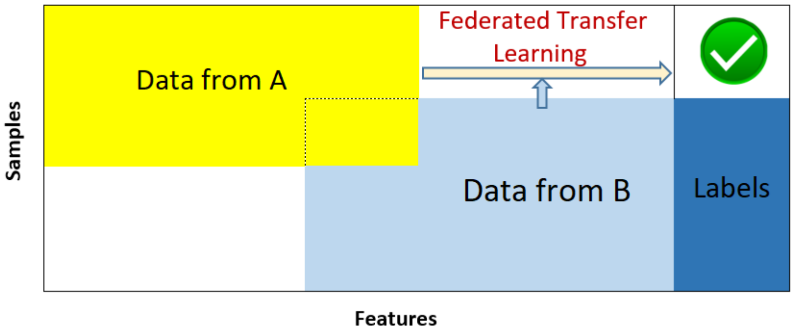

Figure 4: Federated Transfer Learning

### 4.2 Problem Formulation

From equation (1) we can calculate the Weighted Average of model parameters in Federated Learning.

$$w_{t+1} = \sum_{k=1}^{k} \frac{n_k}{n} w_{t+1}^{k} \tag{1}$$

## 5 Discussion

### 5.1 Challenges

- **Client-related Challenges :** Clients are viewed as independent under the FL paradigm, which means they are able to complete the majority of tasks on their own. As a result, they have the option to exit the system at any time, which might delay convergence and interfere with the training process [16]. In FL, preventing client dropouts is a never-ending task. In addition, choosing clients who can provide quality models and data is a crucial task. Sometimes, clients create bots together to engage in any form of harmful activity, rendering All outcomes from the training process unreliable. Several client-related issues impair FL's performance.

- **Training-data-related Challenge :** The training data are essential in the FL paradigm since they impact how well FL models perform. Regarding data quality, there are several issues to consider. Another pressing issue in the FL paradigm is the privacy of the training data [5]. The FL paradigm is currently facing a number of technological hurdles because to the non-iid. nature of the training data, and a solution is now more crucial than ever. One of the biggest issues is also ensuring the data's quality and preventing it from polluting the paradigm [15]. Strong solutions are required for the issues associated with training data in order to fully utilise FL's potential.

- **Privacy concerns Challenge :** Finally, in federated learning applications, anonymity is frequently a top priority. By exchanging model changes, such as gradient information, rather than the raw data, federated learning takes a step towards preserving the data created on each device. The central server or a third party may learn sensitive information if model updates are communicated during the training process [12]. Although modern approaches use technologies like secure multiparty computation (SMC) or differential privacy to increase the privacy of federated learning, these methods frequently sacrifice model performance or system efficiency to achieve privacy [2] [12]. Realizing private federated learning systems is a significant theoretical and practical challenge in terms of comprehending and balancing these tradeoffs.[9]

### 5.2 Future Development of Federated Learning :

Robotics and autonomous systems have several potential uses for federated learning, which enables dispersed machine learning across various devices and systems without centralised data storage. The following are some potential directions for federated learning in robotics and autonomous systems in the future: Robotic collaboration in learning: Teams of robots can learn from one another's mistakes and experiences, enhancing their performance as a whole. Federated learning can make such collaboration possible while protecting the confidentiality of the data that each robot collects. Learning at the edge for autonomous systems Federated learning can be used to do training at the edge for autonomous systems, such as drones or self-driving automobiles, eliminating the need to send massive volumes of data to a centralised server. This can aid in lowering latency and increasing overall effectiveness of the system.

  - **Extreme communication schemes :** We still don't know how much communication federated learning will demand. A lack of precision may be accepted by machine learning optimization algorithms; in fact, this flaw may promote generalisation [19]. Research on traditional data centre communication technologies, such as one-shot or divide-and-conquer [11], but it is unknown how these strategies would behave in vast and very heterogeneous networks.

– **Beyond supervised learning :** It's critical to keep in mind that the approaches outlined up to this point were created with the job of supervised learning in mind, which means they make the assumption that labels are present for all of the data in the federated network. In actuality, a large portion of the data produced by realistic federated networks might be poorly or unlabeled. However, the issue at hand might not be fitting a model to the data, as shown in [1], but rather performing some exploratory data analysis, figuring out aggregate statistics, or carrying out a more difficult task, like reinforcement learning. In federated networks, problems outside supervised learning will probably call for comparable solutions to scalability, heterogeneity, and privacy issues.

# 6 Conclusion

FL is recognized for its innovative approach to addressing these issues.Federated learning has emerged as a promising approach for enabling collaborative learning in distributed and privacy-sensitive settings, including robotics and autonomous systems. Previous studies have shown that federated learning is feasible and beneficial in various application domains such as object recognition, navigation, and control. However, there are still several challenges that need to be addressed to fully realize the potential of federated learning in robotics and autonomous systems. These challenges include scalability, communication efficiency, model robustness, and security. Despite these challenges, recent advancements in federated learning techniques and the increasing availability of large-scale and diverse datasets provide hope for the future of federated learning in robotics and autonomous systems. It is expected that federated learning will play a critical role in enabling intelligent and autonomous systems to learn from distributed and diverse data sources while preserving data privacy and security, and advancing the state of the art in robotics and autonomous systems.

# References

[1] Naman Agarwal, Ananda Theertha Suresh, Felix Xinnan X Yu, Sanjiv Kumar, and Brendan McMahan. cpsgd: Communication-efficient and differentially-private distributed sgd. *Advances in Neural Information Processing Systems*, 31, 2018.

[2] Keith Bonawitz, Vladimir Ivanov, Ben Kreuter, Antonio Marcedone, H Brendan McMahan, Sarvar Patel, Daniel Ramage, Aaron Segal, and Karn Seth. Practical secure aggregation for privacy-preserving machine learning. In *proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, pages 1175–1191, 2017.

[3] Minghong Fang, Xiaoyu Cao, Jinyuan Jia, and Neil Zhenqiang Gong. Local model poisoning attacks to byzantine-robust federated learning. In *Proceedings of the 29th USENIX Conference on Security Symposium*, pages 1623–1640, 2020.

[4] Juan Jose Gamboa-Montero, Fernando Alonso-Martin, Sara Marques-Villarroya, Joao Sequeira, and Miguel A Salichs. Asynchronous federated learning system for human–robot touch interaction. *Expert Systems with Applications*, 211:118510, 2023.

[5] Meng Hao, Hongwei Li, Xizhao Luo, Guowen Xu, Haomiao Yang, and Sen Liu. Efficient and privacy-enhanced federated learning for industrial artificial intelligence. *IEEE Transactions on Industrial Informatics*, 16(10):6532–6542, 2019.

[6] Christian Koetsier, Jelena Fiosina, Jan N. Gremmel, Jörg P. Müller, David M. Woisetschläger, and Monika Sester. Detection of anomalous vehicle trajectories using federated learning. *ISPRS Open Journal of Photogrammetry and Remote Sensing*, 4:100013, 2022.

[7] Jakub Konečný, H. Brendan McMahan, Felix X. Yu, Peter Richtarik, Ananda Theertha Suresh, and Dave Bacon. Federated learning: Strategies for improving communication efficiency. In *NIPS Workshop on Private Multi-Party Machine Learning*, 2016.

[8] Li Li, Yuxi Fan, Mike Tse, and Kuo-Yi Lin. A review of applications in federated learning. *Computers & Industrial Engineering*, 149:106854, 2020.

[9] 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.

[10] Jiaming Liu and Zhi Zheng. A path planning method based on collaborative learning for multi-robot with connectivity and obstacle avoidance constraints. In *2022 China Automation Congress (CAC)*, pages 6770–6775, 2022.

[11] Lester Mackey, Michael Jordan, and Ameet Talwalkar. Divide-and-conquer matrix factorization. *Advances in neural information processing systems*, 24, 2011.

[12] H Brendan McMahan, Daniel Ramage, Kunal Talwar, and Li Zhang. Learning differentially private recurrent language models. *arXiv preprint arXiv:1710.06963*, 2017.

[13] Dinh C Nguyen, Ming Ding, Pubudu N Pathirana, Aruna Seneviratne, Jun Li, and H Vincent Poor. Federated learning for internet of things: A comprehensive survey. *IEEE Communications Surveys & Tutorials*, 23(3):1622–1658, 2021.

[14] Sudipan Saha and Tahir Ahmad. Federated transfer learning: concept and applications. *Intelligenza Artificiale*, 15(1):35–44, 2021.

[15] Vale Tolpegin, Stacey Truex, Mehmet Emre Gursoy, and Ling Liu. Data poisoning attacks against federated learning systems. In *Computer Security–ESORICS 2020: 25th European Symposium on Research in Computer Security, ESORICS 2020, Guildford, UK, September 14–18, 2020, Proceedings, Part I 25*, pages 480–501. Springer, 2020.

[16] Wentai Wu, Ligang He, Weiwei Lin, and Rui Mao. Accelerating federated learning over reliability-agnostic clients in mobile edge computing systems. *IEEE Transactions on Parallel and Distributed Systems*, 32(7):1539–1551, 2020.

[17] Yu Xianjia, Jorge Pena Queralta, Jukka Heikkonen, and Tomi Westerlund. Federated learning in robotic and autonomous systems. *Procedia Computer Science*, 191:135–142, 2021.

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

[19] Yuan Yao, Lorenzo Rosasco, and Andrea Caponnetto. On early stopping in gradient descent learning. *Constructive Approximation*, 26(2):289–315, 2007.

[20] Hangyu Zhu, Haoyu Zhang, and Yaochu Jin. From federated learning to federated neural architecture search: a survey. *Complex & Intelligent Systems*, 7:639–657, 2021.