Federated Learning-based neural networks for autonomous driving

Tingyu Ma

College of Science and Engineering, University of Glasgow, Glasgow G12 8QQ, United Kingdom

2572228M@student.gla.ac.uk

Abstract. An emerging technology with the capacity to revolutionize the transportation sector is autonomous driving, offering the promise of heightened safety, efficiency, and convenience. However, the widescale deployment of autonomous vehicles presents a multitude of challenges, notably the necessity for robust and adaptable machine learning (ML) models capable of handling a wide array of dynamic real-world scenarios. Enter Federated Learning (FL), a decentralized ML approach that has gained recognition as a potential solution to these challenges. This paper delves into the primary advantages of FL within the context of autonomous driving. It highlights FL's capacity to seamlessly adapt to edge devices, respond to localized changes, and continually enhance safety and performance. The document substantiates these advantages through numerous case studies and empirical evidence, demonstrating how FL can potentially elevate the vision, decision-making, control systems, data transmission, and learning model capabilities of autonomous vehicles. By harnessing the collective intelligence of autonomous vehicles while preserving data privacy and security, FL holds the potential to propel us closer to a future where safe, efficient, and autonomous transportation becomes an attainable reality.

Keywords: Federated Learning, Machine Learning, Autonomous Driving, Edge Devices, Deployment.

1. Introduction

In an era characterized by swift advancements in information and communication technology, accompanied by the exponential expansion of data resources and computational capabilities, the task of amassing vast datasets has become more accessible than ever. This technological progress has led to a significant interest in ML by major corporations, such as Tesla in the automotive sector. One of the prominent areas of focus is autonomous driving, which has propelled the emergence of the concept known as Vehicle Edge Computing Networks (VECN) [1].

However, with the increasing data stored on edge devices, the limitations of traditional ML frameworks have become evident. These challenges encompass issues like high communication overhead, concerns about user data privacy, efficiency of centralized server training, and ensuring compatibility of models [2, 3]. Considering the pivotal role of autonomous driving, even a minor flaw in the acquired model can lead to significant repercussions. The constraints of finite resources and the imperative for swift responses pose challenges for central servers aiming to train exceptionally precise models for autonomous driving. Moreover, sharing driving data frequently and extensively raises valid worries about privacy breaches and data leaks. As a result, developing an accurate and privacy-respecting learning approach for autonomous driving has become a central challenge in this field.

The concept of Federated Learning (FL) gained prominence around recently, with Google researchers, including McMahan et al., introduced the idea of training ML models across multiple devices while keeping the data localized [4]. This approach aims to tackle issues related to privacy and the limitations of communication bandwidth that arise with centralized data storage. FL is a technology or method that permits model training across various servers or devices, without the need to centralize the data. In situations where data privacy and security are crucial, this approach is especially useful since it prevents the transmission of sensitive data to a centralised server. Instead of this, the only information transferred between the central server and individual devices are model updates or gradients. This preserves user data privacy while harnessing the collective power of diverse datasets. FL holds great promise for the field of autonomous driving. However, implementing effective and reliable learning systems in a decentralized manner presents challenges for enterprises [5]. FL also presents its own set of challenges, including ensuring model convergence, dealing with communication delays, and addressing imbalances arising from isolated data sources [6].

Due to the various advantages and disadvantages of FL described above, the opportunities for the use of this technology are expected to greatly increase. However, many companies are not yet ready to adopt this powerful technology, and most still rely on traditional centralized ML, which has its limitations. On one hand, its security is not guaranteed, as malicious user data uploads can impact the entire model. On the other hand, there are challenges related to training, such as the iterative communication overhead, device heterogeneity in learning, and user adoption in system deployment.

This review paper aims to provide a comprehensive exploration of the applications of both traditional ML and FL in relevant scenarios, along with an in-depth analysis of the challenges and potential improvements pertaining to FL techniques. This encompasses aspects such as the security, privacy, and efficiency of existing federated algorithms, all with the goal of establishing dependable and suitable learning and deployment approaches in the context of vehicular environments. The paper also outlines potential avenues for future research in the FL domain, offering conceptual insights to inspire further investigation.

2. Method

2.1. Overview of FL

As opposed to the conventional practice of centralizing data on a single server or in the cloud, Federated Learning (FL) represents a machine learning approach that facilitates model training across a diverse array of decentralized edge devices. These devices can include smartphones, IoT devices, or local servers, all while preserving the data directly on these endpoints. This approach proves especially valuable in scenarios where data privacy and security are paramount concerns, as it allows for collaborative model training without the need to expose the underlying raw data [4, 7]. Figure 1 shown a representation of FL. FL has primarily 8 steps: 1) Initialization: A global ML model is initialized on a centralized server or in the cloud. The model serves as the starting point for the FL process. 2) Device Selection: It is decided which clients or edge devices will take part in the learning model process. These devices have local data that can be used for model training. 3) Model Distribution: The first selected devices receive the global model. The model is then updated by each device using local data. 4) Local Model Training: On each device, the local model is fine-tuned using the data available locally. This may involve running multiple rounds of training iterations (e.g., gradient descent) on the local data to improve the model's accuracy. 5) Model Update Aggregation: After local training, each device sends its new model parameters updates (e.g., gradients) back to the central server or aggregator without sharing the raw data. These updates are aggregated in some way to renew the global model. 6) Global Model Update: The centralized server aggregates the model updates from all participating devices, typically by performing some form of weighted averaging. The global model is then updated with the aggregated updates. 7) Iteration: Steps 3 to 6 are repeated for multiple rounds or iterations, allowing the global model to gradually improve through collaborative learning from different devices. 8) Evaluation and Deployment: The final global model can be evaluated for performance and, if satisfactory, deployed for use in the application or service it was designed for.

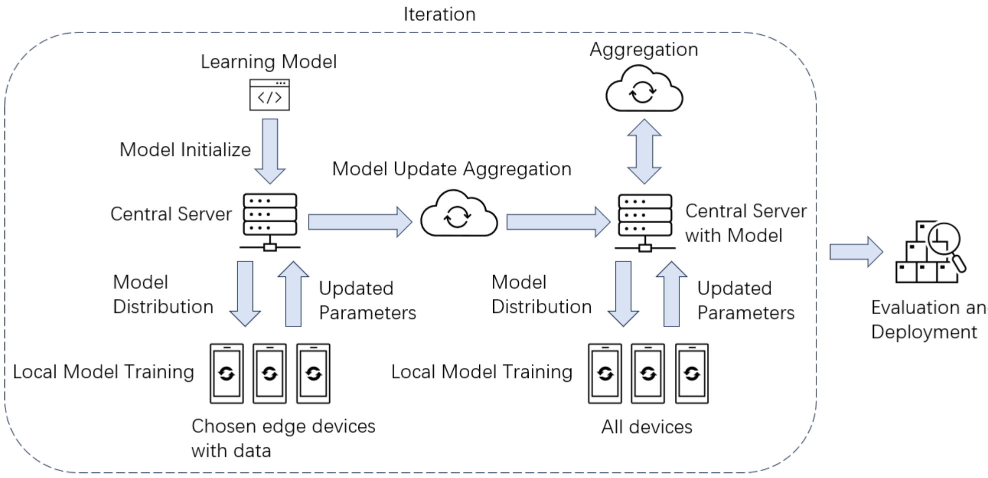

Figure 1. Federated Learning Deployment.

2.2. Recognize Different FLs

FL can be categorized into various types, each with its own focus and use cases. Three common types of FL are:

2.2.1. Horizontal FL

A collaborative method called horizontal FL protects privacy in situations where different entities have datasets with comparable characteristics, but they are reluctant to openly exchange their individual data. In this setting, an ML model is collaboratively trained by a number of participants using their respective data samples, all of which share a common or closely aligned feature space. Instead of directly sharing their raw data, these parties opt for a collaborative process that often involves aggregating or averaging local updates to refine the shared model. For instance, this could apply to situations where different mobile devices collect user behavior data independently, and the device owners wish to maintain data privacy while deriving collective insights through ML [8].

2.2.2. Vertical FL

Vertical FL serves as a crucial framework for facilitating privacy-preserving collaboration among multiple entities, particularly in cases where they possess complementary datasets that feature shared identifiers. This collaborative approach becomes essential when these parties are reluctant to divulge the entirety of their data. For example, consider a scenario where a hospital maintains patient demographic information, while a research institution possesses detailed patient medical records. Vertical FL enables these organizations to work together on an ML task without compromising the confidentiality of sensitive patient information. This collaborative process entails training ML models using data that share common keys or identifiers while safeguarding the privacy of non-shared data elements. In essence, it empowers diverse entities to harness the insights derived from their collective data resources while upholding stringent data protection and privacy standards [9].

2.2.3. Transfer FL

Transfer FL is a specialized approach focused on the crucial task of transferring and adapting ML models across diverse edge devices or environments. It finds its significance in scenarios where there is a need to tailor a model to accommodate variations or constraints specific to local settings. In essence, Transfer FL seeks to transfer knowledge and expertise acquired from one source, such as a central model or a well-established device, to another. This approach becomes particularly valuable when an ML model must adjust and fine-tune its performance to cater to the unique characteristics of various edge devices or environments. For instance, consider a language translation model that has been initially trained on a high-performance device. Transfer FL can be employed to further enhance its translation capabilities on another device, perhaps one with limited data connectivity. By adapting the model to the specific constraints and requirements of this device, it ensures more effective and context-aware translation performance. Importantly, Transfer FL retains the valuable knowledge gained during the initial training phase, making it a powerful tool for optimizing ML models across diverse settings [10, 11].

These three varieties of FL demonstrate FL's adaptability to different data-sharing settings and privacy concerns while facilitating collaborative ML. Each type addresses specific challenges and can be applied in different real-world situations, making FL a powerful technique for privacy-preserving and decentralized ML.

2.3. Federated Algorithms Security

FL is a distributed ML technique designed to protect clients' private data while collaboratively training a shared model. However, even FL can leak information through the analysis of model parameters shared by clients. To enhance privacy in FL, a fresh strategy dubbed Noising before Model Aggregation Federated Learning (NbAFL) is proposed [12]. Before aggregation, NbAFL adds synthetic noise to client parameters, ensuring differential privacy at various protection levels by adjusting the noise variance. The paper establishes a theoretical convergence bound for NbAFL, revealing key insights: 1) a tradeoff between convergence and privacy; 2) improved convergence with more participating clients; 3) an optimal number of aggregation rounds for specific privacy levels. A random client selection strategy (K-client) is introduced, offering similar advantages, with an optimal K for achieving the best convergence at a given privacy level. Theoretical findings align with simulation results, offering valuable guidance for designing FL systems with improved privacy and convergence tradeoffs.

2.4. Federated Algorithms Privacy

In the context of Vehicular Edge Computing (VEC), privacy concerns have become increasingly prominent, especially in the field of autonomous driving. To address these privacy challenges, FL, a privacy-preserving strategy pioneered by Google, is being applied to VEC. This approach allows original data to remain on individual vehicles while sharing only model parameters through Mobile Edge Computing (MEC) servers. Unlike previous studies that assumed honest MEC servers and vehicles, this research considers the presence of malicious actors [13]. First, a traceable identity-based privacy preservation system is suggested for scenarios involving malevolent vehicles and honest-but-curious MEC servers. For increased security, it uses a blockchain-based Reputation-based Incentive Autonomous Driving Mechanism (RIADM) and an upgraded Dijk-Gentry-Halevi-Vaikutanathan (DGHV) algorithm. Secondly, for situations where both parties are untrustworthy (semi-honest MEC servers and malicious vehicles), to safeguard vehicle IDs, a Zero-Knowledge Proof (ZKP) anonymous identity-based privacy approach is created. Simulation results, based on the photographs of actual roads, show the viability of the suggested plan. It reduces training loss in autonomous driving by about 70%, increases accuracy by approximately 5%, all while maintaining robust privacy in the face of dishonest MEC servers and vehicles.

2.5. Federated Algorithm Efficiency

In order to show the advantages of FL in terms of actual operating efficiency, it is necessary to compare it with CL. The potential of FL and CL in terms of distributing load in mobile networks and how the exchange of model parameters in FL and the exchange of training data in CL varies, especially in terms of mobility, is an untapped area. Drainakis et al. directly developed a practical system model and a realistic evaluation environment, and a practical system model created to assess and contrast FL and CL ML fusions in relation to network resource use, energy efficiency, and real-world conditions, including bandwidth availability, user mobility, data availability, and client selection [14]. Existing studies often address these aspects individually or in a limited scope. The system uses AI/ML software for accurate ML process replication, real-world motion tracking to capture user movement patterns, and models based on accurate measurements for bandwidth availability. This comprehensive approach provides valuable insights into the performance of FL and CL in dynamic mobile networks, not just privacy considerations.

3. Applications and discussion

3.1. FL in Vehicular Networks

Vehicular networks, often referred to as V2X (Vehicle-to-Everything) networks, encompass various communication scenarios involving vehicles, infrastructure, and other road users. FL can be applied in Vehicular networks in several ways. Elbir et al. studied and discussed the main challenges of FL-related data heterogeneity, privacy, control, and resource use through data generated from lidar and the detection of some 3D objects [15].

3.1.1. Data

In order to improve the accuracy of the present autonomous driving model, data collection at a central local server can help, but due to the sharing of personal privacy, this method seriously violates the user's privacy right. A new federal autonomous driving network was designed [16]. In the research, a new method, called Peer-to-Peer Deep Federated Learning (DFL), is introduced without the need for central control, specifically enhancing model stability, convergence, and dealing with the difficulties associated with unbalanced data distribution. From the experimental results, the use of FADNet and DFL developed by the team has superiority and higher accuracy. What's more, the approach also takes into account user privacy concerns, ensuring that sensitive information remains distributed and confidential by avoiding user data collection into centralized servers.

3.1.2. Application

FL still has some technical and system deployment challenges in actual use. Zhang et al. directly used a realistic industrial autonomous driving use case, wheel deflection [17]. In order to effectively train learning models in decentralised distributed contexts, they offer an end-to-end FL strategy. The model accuracy, training efficiency and consumption of transmission resources of traditional CL and FL are compared and discussed. The final result shows that end-to-end FL outperforms centralized learning by reducing training time and bandwidth costs while maintaining model accuracy. It leverages model sharing between edge vehicles to enhance global knowledge. This approach goes beyond autonomous vehicle applications to benefit resource-constrained edge devices for tasks such as camera sensors and adapt to changing environments. However, synchronization limitations in heterogeneous hardware and network environments have prompted the study of asynchronous aggregation protocols to address real-world scenarios.

3.2. Discuss

FL offers a promising approach to train autonomous driving models while addressing critical concerns such as data privacy and distributed data heterogeneity. It enables efficient model training, reduces bandwidth usage, and can adapt to dynamic driving conditions, making it a valuable tool in the development of autonomous vehicles and vehicular networks. However, it's essential to continue researching and refining FL techniques to overcome deployment challenges and ensure its effectiveness in complex, real-world scenarios.

4. Conclusion

This article outlines the differences and advantages/disadvantages between FL and centralized learning. Through an in-depth exploration of existing literature and research in this field, it is evident that FL has emerged as a promising transformative technology for enhancing the safety, efficiency, and overall performance of autonomous vehicles. FL addresses key challenges such as data privacy, scalability, and real-time decision-making, making it an ideal solution for autonomous systems that rely on collecting vast amounts of data from diverse sources. It enables collaborative training of ML models on distributed edge devices while preserving data locality, potentially accelerating the development and deployment of autonomous vehicles. However, it's important to recognize that within the context of autonomous driving, Federated Learning (FL) remains a relatively nascent field, characterized by various technical and practical challenges. Many of these technologies are predominantly theoretical, and their practical implementation presents substantial hurdles. These challenges encompass the optimization of communication protocols, the establishment of resilience against adversarial attacks, and the development of standardized frameworks tailored to FL's integration into the automotive industry.

As society progresses toward a future where autonomous vehicles assume a more prominent role in the transportation systems, FL offers a promising avenue. It paves the way for safer, more efficient, and more convenient mobility solutions. Through ongoing research and collaboration between academia and industry, it can be anticipated that continuous strides in FL technology. This evolution is poised to reshape the landscape of autonomous driving, bringing us closer to the realization of fully autonomous and secure transportation systems.

References

[1] Xie R C et al. 2019 Collaborative vehicular edge computing networks: Architecture design and research challenges. IEEE Access 7 (2019): 178942-178952

[2] Drainakis G et al. 2020 Federated vs. centralized machine learning under privacy-elastic users: A comparative analysis. 2020 IEEE 19th International Symposium on Network Computing and Applications (NCA). IEEE

[3] L'heureux A et al. 2017 Machine learning with big data: Challenges and approaches." Ieee Access 5 7776-7797

[4] McMahan B et al. 2017 Communication-efficient learning of deep networks from decentralized data Artificial intelligence and statistics. PMLR

[5] Wang J and Joshi G 2021 Cooperative SGD: A unified framework for the design and analysis of local-update SGD algorithms. The Journal of Machine Learning Research, 22(1), pp.9709-9758

[6] Kairouz P et al. 2021 Advances and open problems in federated learning Foundations and Trends® in Machine Learning 14.1–2 (2021): 1-210

[7] Mammen P M 2021 Federated learning: Opportunities and challenges arXiv preprint arXiv:2101.05428 (2021)

[8] Singh P et al. 2022 Federated learning: Challenges, methods, and future directions Federated Learning for IoT Applications. Cham: Springer International Publishing 199-214

[9] Chen T Y et al. 2020 Vafl: a method of vertical asynchronous federated learning arXiv preprint arXiv:2007.06081

[10] Liu Y et al 2020 A Secure Federated Transfer Learning Framework in IEEE Intelligent Systems, vol. 35, no. 4, pp. 70-82, 1 July-Aug doi: 10.1109/MIS.2020.2988525

[11] Liu Y et al 2020 Privacy-preserving traffic flow prediction: A federated learning approach. IEEE Internet Things J. 7(8), 7751–7763

[12] Wei K et al. 2020 Federated learning with differential privacy: Algorithms and performance analysis IEEE Transactions on Information Forensics and Security 15 3454-3469

[13] Li Y et al. 2021 Privacy-preserved federated learning for autonomous driving IEEE Transactions on Intelligent Transportation Systems 23.7 8423-8434

[14] Drainakis G et al. 2020 Federated vs. centralized machine learning under privacy-elastic users: A comparative analysis 2020 IEEE 19th International Symposium on Network Computing and Applications (NCA). IEEE

[15] Elbir A M et al. 2022 Federated learning in vehicular networks 2022 IEEE International Mediterranean Conference on Communications and Networking (MeditCom). IEEE, 2022

[16] Nguyen A et al. 2022 Deep federated learning for autonomous driving 2022 IEEE Intelligent Vehicles Symposium (IV). IEEE

[17] Zhang H Bosch J and Olsson H H 2021 End-to-end federated learning for autonomous driving vehicles. In 2021 International Joint Conference on Neural Networks (IJCNN) (pp. 1-8). IEEE