Proceedings of the 4th International Conference on Signal Processing and Machine Learning
DOI: 10.54254/2755-2721/51/20241158

Empowering safe and secure autonomy: Federated learning in the era of autonomous driving

Weixi Wang

The Department of Computer Science, Xi'an Jiaotong University, Xi'an, 710049, China

wangweixi@stu.xjtu.edu.cn

Abstract. Artificial Intelligence (AI) has a significant impact on empowering autonomous driving systems to perceive and interpret the environment effectively. However, ensuring data privacy and security in autonomous driving systems is a critical challenge. To surmount these hurdles, federated learning has emerged as an effective strategy. Federated learning is a decentralized machine learning approach that facilitates the cooperative training of models across a diverse set of connected devices, enabling them to collectively learn and improve their performance, while preserving data privacy. This approach eliminates the necessity of sharing raw data and only involves sharing model updates with a central aggregator, thereby ensuring privacy and minimizing data exposure. This paper examines the implementation of federated learning in autonomous driving. It explores the principles of federated learning, including decentralized training, local model updates, model aggregation, privacy preservation, iterative learning, and heterogeneity handling. Two specific approaches, Deep Federated Learning (DFL) and End-to-End Federated Learning, are discussed, highlighting their benefits in enhancing privacy and maintaining prediction accuracy. The paper also discusses the applications of federated learning in communication and control aspects of autonomous driving. It emphasizes the scalability, adaptability, edge computing, real-time learning, federated transfer learning, and privacy-preserving data sharing as potential future prospects for federated learning in autonomous driving. Overall, federated learning offers a unique opportunity to address privacy concerns in autonomous driving systems while harnessing the collective intelligence of a fleet of vehicles. It has the potential to revolutionize the field and contribute to the development of safe and secure autonomous driving technologies.

Keywords: Federated Learning, Autonomous Driving, Artificial Intelligence, Privacy Preserving.

1. Introduction

The field of autonomous driving has garnered significant attention and investment from various companies, driven by the potential to revolutionize transportation systems and enhance road safety [1, 2]. Autonomous driving pertains to the capability of vehicles to operate autonomously, without human intervention. It relies on the utilization of Artificial Intelligence (AI) and advanced sensing technologies to navigate, perceive the environment, and make informed decisions. The application scenarios for autonomous driving are vast, ranging from personal vehicles to public transportation systems and logistics operations.

DOI: 10.54254/2755-2721/51/20241158

Artificial intelligence plays a pivotal role in enabling autonomous driving systems to perceive and interpret the environment effectively. Through techniques e.g. computer vision, sensor fusion, and machine learning, AI algorithms can analyze sensor data from cameras, lidar, radar, and other sources to understand the surrounding objects, road conditions, and potential hazards [3]. The capability to process extensive volumes of data in real-time empowers autonomous vehicles to make precise decisions and respond effectively to dynamic traffic scenarios.

Ensuring data privacy and security in autonomous driving systems presents a significant challenge. Autonomous vehicles gather and analyze massive quantities of sensitive data, such as images, videos, and geolocation information. Protecting this data from unauthorized access and potential misuse is of paramount importance. Traditional centralized approaches, where data is aggregated and stored in a central server, raise concerns about privacy breaches and security vulnerabilities [4].

To surmount these hurdles, federated learning has gained significant attention as a effective strategy. The Deep Federated Learning (DFL) approach effectively addresses privacy concerns by conducting model training on decentralized devices as well as data centers which are isolated, such as autonomous cars. In this approach, data remains localized, indicating that each data silo retains its local data and refrains from directly sharing it. Instead, periodic model updates are transmitted to other silos to facilitate collaborative model training [5]. As a decentralized machine learning approach, federated learning prioritizes data privacy by conducting the learning process locally on individual devices. Instead of sending the original data to a central server, the approach involves sharing only the model updates with a central aggregator.This methodology guarantees that sensitive data remains securely stored on the respective devices.This distributed learning paradigm leverages the collective intelligence of a fleet of autonomous vehicles without compromising data privacy and security. In recent years, several new technologies have been introduced to enhance privacy in autonomous driving. Cutting-edge methods such as secure multi-party computation, differential privacy, and homomorphic encryption offer robust mechanisms to protect data throughout the training and inference stages, ensuring its confidentiality and integrity. These techniques introduce advanced mechanisms for ensuring data protection and privacy [5-7]. These advancements, coupled with the characteristics of federated learning, provide a unique opportunity to address privacy concerns in autonomous driving effectively.

Given the importance of the research and the existing gap in the literature, this review aims to explore the application of federated learning in autonomous driving. This paper will delve into the principles of AI in autonomous driving, discuss the potential applications of AI algorithms in various aspects of autonomous vehicles, and then focus on the concept of federated learning as a solution to privacy concerns. Additionally, the latest technologies and techniques that can be used in conjunction with federated learning were also investigated to uphold privacy as well as security in autonomous driving fields.

2. Method

2.1. Brief Introduction of Federated learning

As a decentralized machine learning approach, federated learning facilitates the cooperative training of models across a diverse set of connected devices, enabling them to collectively learn and improve their performance, ensuring data privacy and security. Unlike traditional centralized machine learning methods that involve collecting and aggregating data on a central server, training process takes place locally on individual devices, which is allowed by federated learning. This decentralized approach eliminates the need to share raw data between devices, preserving data privacy [8].

The idea behind federated learning stems from the recognition that valuable data is often stored on edge devices such as smartphones, Internet of Things (IoT) devices, or autonomous vehicles. These devices generate and amass extensive datasets, but privacy vulnerabilities and substantial bandwidth consumption are inherent when data is transmitted for training purposes to a central server. Federated learning addresses this predicament by relocating the model training process directly to the data sources themselves. Rather than sending data to a central server, the learning algorithm is distributed across

DOI: 10.54254/2755-2721/51/20241158

participating devices. This decentralized approach enables devices to train models using their local data, ensuring that the data remains stored locally. As a result, privacy concerns are minimized, and communication overhead is reduced.

2.2. Principles of Federated Learning

Decentralized Training: Federated learning enables training to take place on individual devices or edge nodes, which have access to local data. By keeping the training process decentralized, federated learning avoids the need for data aggregation in a central server.

Local Model Updates: Each participating device calculates local model updates by leveraging its own data in the process. These updates capture the knowledge gained from the device's data and reflect the device's specific characteristics and data distribution.

Model Aggregation: Upon computation, the local model updates are dispatched to a central aggregator, which consolidates these updates to construct an updated global model. The aggregation process can involve techniques such as weighted averaging, where the contributions of each device are weighted based on factors like data quality or device capabilities.

Privacy Preservation: One of the fundamental principles of federated learning is the preservation of privacy. This approach ensures that the training data remains on the devices, with only the model updates being shared. This methodology guarantees that sensitive data is neither exposed nor transferred, thereby mitigating the risks of data breaches and privacy violations.

Iterative Learning: Federated learning typically involves multiple rounds of local training and model aggregation. The iterative process allows the global model to improve over time as each device's knowledge is combined and shared among the participants.

Heterogeneity Handling: Federated learning accommodates device heterogeneity by considering variations in computational capabilities, data quality, and other relevant factors. Techniques such as adaptive weighting or learning rate adjustments can be employed to account for these differences.

2.3. Deep Federated Learning

Introducing Deep Federated Learning (DFL): A groundbreaking methodology for training autonomous driving policies that places paramount importance on privacy considerations. A fully decentralized, peer-to-peer framework is used to train autonomous driving solutions in the DFL approach. The distributed training process can benefit from this methodology's potential to enhance accuracy and alleviate communication congestion.

Addressing privacy concerns, the DFL approach conducts statistical model training over remote devices or isolated data centers, including autonomous cars, while ensuring data localization. This approach introduces a Federated Autonomous Driving network (FADNet) designed specifically for federated training, with a focus on capturing "line-like" patterns in input frames that guide driving direction. By integrating a decentralized federated learning algorithm with a tailored network architecture, the Decentralized Federated Learning (DFL) approach achieves enhanced precision and mitigates communication congestion in the distributed training process. This combination enables enhanced accuracy by allowing individual nodes to locally train models using their own datasets while selectively exchanging crucial model updates with other nodes. Additionally, the specialized network design optimizes the communication efficiency among the nodes, reducing the overall bandwidth requirements and minimizing potential bottlenecks. As a result, the DFL approach provides a potent solution that harmonizes accuracy and communication efficiency, addressing key challenges in collaborative model training for autonomous driving systems.

The performance of the DFL approach is evaluated using the Root-Mean-Square Error (RMSE) metric and compared to several recent methods. The results demonstrate that the DFL approach outperforms the most advanced methods available, while simultaneously maintaining strict user data privacy.

DOI: 10.54254/2755-2721/51/20241158

2.4. End-to-End Federated Learning

This paper introduces a novel approach to federated learning for machine learning tasks performed directly on the devices, with a primary emphasis on the prediction of steering angles in autonomous vehicles The approach involves incorporating a two-stream deep Convolutional Neural Network (CNN) architecture and distributing the dataset to edge devices, creating an emulation of an on-device data environment. The dataset is divided into relevant segments and transmitted to edge devices, with each segment comprising a sequence of consecutively ordered video frame images. By leveraging future driving data, the models undergo continual training using captured data, enabling them to make predictions and validate the information pertaining to steering wheel angles.

The primary concept of this approach revolves around leveraging Federated Learning to train machine learning models on edge devices. This strategy aims to minimize training time and bandwidth costs while upholding prediction accuracy. The research paper further delves into the utilization of advanced neural networks in conjunction with Federated Learning. It also explores the identification of appropriate aggregation algorithms and protocols to suit diverse real-world industrial scenarios within the proposed approach.

This approach adheres to certain principles, such as on-device Machine Learning to enhance privacy and minimize latency, along with the utilization of Federated Learning to facilitate distributed learning without necessitating centralized data storage. The paper also emphasizes the importance of validating the approach in real-world industrial scenarios and exploring more advanced neural networks and aggregation algorithms to improve the approach's effectiveness.

3. Applications and discussion

3.1. Communication

Federated learning eliminates the necessity for individual vehicles to directly share their data with each other or upload sensitive information to a common server. Each vehicle only needs to regularly update the parameters in the autonomous driving model, which makes it more private and safer. In other words, in contrast to other approaches that prioritize enhancing the reliability of autonomous driving solutions at the expense of user privacy, the Federated Learning (FL) approach prioritizes privacy concerns by conducting model training on distributed devices or isolated computing facilities, such as autonomous cars. This methodology ensures that data remains localized, safeguarding user privacy throughout the training process.

3.2. Control

Federated learning enables multiple Connected and Autonomous Vehicles (CAVs) [9] to train individual machine learning models locally, leveraging their unique datasets, which can be limited due to on-chip memory constraints. The individual models are subsequently transmitted to a central server, where they are consolidated to formulate a global model that can be utilized by all CAVs. This approach has several benefits for improving the performance of autonomous controllers for CAVs. For example, it can effectively address the constraints associated with local data storage and enhance the precision and resilience of the autonomous controller's performance across diverse road conditions and traffic scenarios. Additionally, it can help reduce the risk of overfitting to local data and improve the generalization of the controller to new environments [10].

3.3. Future Prospect

The application of federated learning in autonomous driving opens up promising future prospects. Some potential areas of development are provided as below:

a) Scalability and Adaptability: Federated learning allows autonomous driving systems to scale efficiently, accommodating a large number of vehicles and edge devices. As the number of connected vehicles increases, federated learning can adapt to the growing network, enabling collaborative learning without compromising privacy and communication efficiency.

DOI: 10.54254/2755-2721/51/20241158

b) Edge Computing and Real-time Learning: With the advancement of edge computing capabilities, federated learning can be integrated with edge nodes in autonomous vehicles. This enables real-time learning and decision-making, reducing the reliance on centralized servers and minimizing communication delays. By leveraging the computational power at the edge, autonomous vehicles can continuously improve their models and adapt to changing road conditions in real-time.

c) Federated Transfer Learning: Federated transfer learning amalgamates the advantages of both federated learning and transfer learning. Pretrained models or knowledge from one vehicle can be transferred to other vehicles in a federated learning setting, allowing for faster convergence and improved performance across the fleet. This approach reduces the need for extensive training on individual vehicles and promotes knowledge sharing among the networked vehicles.

d) Privacy-Preserving Data Sharing: Federated learning can facilitate secure and privacy-preserving data sharing among autonomous vehicles. Instead of sharing raw data, vehicles can share model updates or aggregated statistics, enabling collaborative learning without compromising individual privacy. This opens up possibilities for cooperative perception, where vehicles collectively improve their perception capabilities by fusing data from multiple sources while preserving privacy.

4. Conclusion

This paper has explored the application of federated learning in autonomous driving. Various methods, such as decentralized training and model aggregation have been investigated, while preserving data privacy through techniques like secure computation and differential privacy. In addition, this paper also discussed potential applications in communication and control aspects, highlighting scalability and real-time learning capabilities. However, challenges persist, including model heterogeneity and fairness. Looking ahead, promising advancements in technologies like 5G and edge computing, coupled with the establishment of standardized protocols, offer great potential for the advancement and widespread adoption of federated learning in the context of autonomous driving. Overall, federated learning presents a viable solution to privacy concerns while fostering collaborative intelligence, thereby paving the way for enhanced efficiency and safety in autonomous driving systems.

References

[1] Ma Y Wang Z Yang H and Yang L 2020 Artificial intelligence applications in the development of autonomous vehicles: a survey in IEEE/CAA Journal of Automatica Sinica vol. 7 no. 2 pp. 315-329 doi: 10.1109/JAS.2020.1003021.

[2] Crayton T J and Meier B M 2017 Autonomous vehicles: Developing a public health research agenda to frame the future of transportation policy J. Transp. Health vol. 6 pp. 245–252

[3] Joel J et al 2017 Computer Vision for Autonomous Vehicles: Problems, Datasets and State-of-the-Art arXiv:1704.05519.

[4] Ekim Y et al 2019 A Survey of Autonomous Driving: Common Practices and Emerging Technologies arXiv: 1906.05113

[5] Anh N et al 2021 Deep Federated Learning for Autonomous Driving arXiv:2110.05754

[6] Bresson G et al 2017 Simultaneous Localization and Mapping: A Survey of Current Trends in Autonomous Driving in IEEE Transactions on Intelligent Vehicles vol. 2 no. 3 pp. 194-220 doi: 10.1109/TIV.2017.2749181

[7] Zhang H J et al 2021 End-to-End Federated Learning for Autonomous Driving Vehicles International Joint Conference on Neural Networks (IJCNN) Shenzhen China pp. 1-8 doi: 10.1109/IJCNN52387.2021.9533808.

[8] Lim W Y B Luong N C Hoang D T 2020 Federated learning in mobile edge networks: A comprehensive survey IEEE Communications Surveys & Tutorials

[9] Han J Ju Z Chen X Yang M Zhang H Huai R 2023 Secure Operations of Connected and Autonomous Vehicles IEEE Transactions on Intelligent Vehicles

[10] Zeng T C et al 2021 Federated Learning on the Road: Autonomous Controller Design for Connected and Autonomous Vehicles arXiv:2102.03401