Federated Learning for Traffic Flow Prediction

Rakshith Ravi
Masters in AI Engineering of Autonomous Systems
Technische Hochschule Ingolstadt
Ingolstadt, Germany
rar5407@thi.de

***Abstract*— Centralized traffic flow prediction methods usually have high accuracy based on the large datasets utilized by them, but they are also at an inherent risk of privacy breaches, since they require individual organizations to collect raw traffic data from multiple distributed organizations and group them. This is problematic due to the growing concern of data privacy and regulations about data usage. In response, a solution is to conduct Federated Learning (FL). FL allows multiple organizations that retain their data to perform collaborative training of prediction models while never sharing the raw data. As a result, FL assists an organization in gaining the advantages of collaborative learning, while there is still the inherent requirement for data isolation of the raw data and without the added protection from sending sensitive data just to get predictions. Additionally, FL reduces the added workload of having to collect and send large data files. However, applying FL to traffic prediction is not without obstacles, most notably data heterogeneity, where share traffic patterns and underlying data distributions differ greatly by client and location. Data that is non-independent and identically distributed (non-IID) can negatively influence the global model's performance. Researchers have developed numerous FL models for traffic prediction. For instance, FedGRU showed similar performance to centralized GRU models, with the added benefit of data privacy. Recent models including FLSTAGCN utilize spatio-temporal graph neural networks with improved attention mechanisms and have prediction performance comparable to or better than centralized advanced spatio-temporal models on real datasets, while preserving the privacy and security of traffic data. Research is ongoing to further refine FL and combat heterogeneity, while providing more efficient communication.**

***Index Terms*—** Federated Learning, Traffic Flow Prediction, Privacy Protection, Spatio-Temporal, Spatial-Temporal, Graph Neural Networks (GNNs), Graph Convolutional Networks (GCNs), Personalized Federated Learning, Communication Efficiency, Non-IID Data, Data Heterogeneity, Aggregation, Synthetic Data Augmentation.

I. INTRODUCTION

Traffic flow prediction is a key part of urban planning and traffic control as they develop smart cities [7]. Understanding traffic flow to gauge city growth and changes of land use would allow the planners to identify which areas are experiencing city development and what are the impacts on land use [7]. This can help planners alter land uses and urban development in sustainable cities. The flow of traffic can provide us insights into demographics and temporal ("when") of human activity patterns - this will give us information for the spatial (where) and temporal aspects of urban planning and land monitoring using traffic as an important indicator. Beyond planning, traffic prediction can help traffic management centres and operators to manage traffic flow, prevent congestion and optimize traffic network performance. Real-time traffic prediction can offer roadway users and businesses legitimate planning information to make travel decision and allow for rerouting when appropriate. It is a critical function of Intelligent Transportation Systems (ITS) and is essential for subsystems such as advanced traveller information, online car-hailing, and traffic management systems [1].

Fig. 1. Smart city traffic environment with connected vehicles and real-time data flow. Source: This image is generated from Leonardo.AI

Traditionally, obtaining accurate predictions of traffic flows has relied heavily on centralized machine learning techniques, emphasized using deep learning models. Although they can show exceptional effectiveness performance, training a deep learning model needs many samples from data collected from a central, pooled data. Unfortunately, this approach still raises concern and can be challenging due to data privacy and security. Traffic data such as that produced through intersection cameras or collected from an invasion of GPS directions can contain sensitive data, such as license plates, vehicle locations, and travel trajectories, which may leak confidential data, creating risks [1]. Direct sharing of traffic data between cities and organizations or pooling that data centrally to train models creates concerns about the privacy of users. In addition, data privacy policies are becoming stricter. Whether in Europe, through the General Data Protection Regulation (GDPR), or the California Consumer Privacy Act (CCPA) in the USA, data privacy has increasingly high stakes that cannot be overlooked when adopting a predictive model of traffic flows. Currently, cities

and public data organizations are subject to very high levels of confidentiality, which prohibit them from sharing data, thus leading to challenges to utilize dataset coming from a single public agency problematic for obtaining predictive analytics at a sufficient level of excellence. This highlights the urgent need for methods that can train powerful prediction models, while protecting data privacy[10].

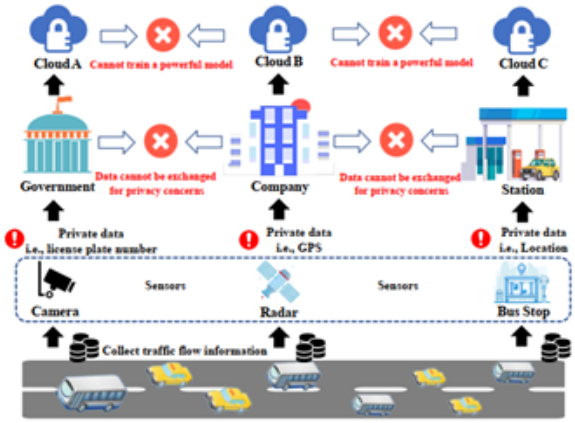


Fig. 2. Privacy and security problems in traffic flow prediction. Source: This image is taken as reference from [1]

In response to these challenges, the idea of Federated Learning (FL), as a privacy-preserving machine learning paradigm, was developed. FL enables multiple participants (referred to as clients, or organizations), who each have their own local data, to collaborate in training a shared global model without exchanging their raw data [7] . Clients first train their models locally, and optionally evaluate their model withheld-out validation or test data, and then forward updated model parameters or gradients to a central server, where these parameters are aggregated. The aggregation results in a new global model, which is sent back to the clients for further training. The distributed training architecture of FL actively mitigates data privacy and security challenges by allowing models to learn from all the combined data from the participants, without having access to individual data points [6].

Although FL presents many benefits for privacy-preserving collaborative training, its application to traffic flow prediction is still an emerging area compared to other applications [14]. The existing body of literature on FL-based traffic prediction is considered minimal and early-stage. This is presented as a research gap, as many of the previous work on FL were in applications such as healthcare and finance [14].

There are several challenges posed by applying FL to traffic flow prediction. The data is highly heterogeneous (non-IID) and comes with complex spatio-temporal dependencies [18]. Simply aggregating models, such as federated averaging (FedAvg), doesn't work well because it doesn't capture the nuanced spatial and temporal correlations in traffic networks, resulting in a global model that does not perform well because it hasn't learned the relationship between the various client data characteristics. Additionally, traffic is dynamic and may change suddenly due to unpredicted conditions, leading to concept drift, where the distribution of incoming real-time traffic data significantly differs from the historical data used in the global model. Classical batch learning processes (and many non-streaming FL processes), typically assume static models pretrained in future data that may turn stale in dynamic and concept drift situations. This is an active research area to effectively capture complex spatio-temporal dependencies, address data heterogeneity, and respond to concept drift in a resource-efficient and privacy-preserving way in an FL framework adapted for traffic data [16].

TABLE I
OVERVIEW OF FEDERATED LEARNING APPLICATIONS ACROSS DOMAINS

Domain	Use Case	Citation
Healthcare	COVID diagnostics, patient monitoring	[11]
Finance	Fraud detection, risk modeling	[11]
Transportation	Traffic flow prediction (early stage)	[2]

This paper aims to address these gaps in research by reviewing the existing FL architectures to address traffic flow prediction problems. We examine various architectures proposed for this use case including GRU's based models called FedGRU [7], GCN based models like FCGCN [2], and frameworks which use auxiliary methods like attention alongside coupling GNN and GRU (FLSTAGCN and Fed-STN) [5]. We also examine how these models are trying to uncover the complex spatio-temporal correlations of traffic data, while also trying to preserve privacy. Additionally, we will examine innovations which address weaknesses such as the impact of data heterogeneity[18], overhead communication [13], and the need for real-time model adjustment to keep up with the concept drift (for example FedOSTC and REFOL) [16]. This paper seeks to give a full overview and analysis of these existing FL based frameworks related to traffic prediction, point out the contributions these publications offer, identify the future plans for FL in the area of traffic prediction, and suggest potential research directions for developing a better, and a truly adaptive privacy-preserving, intelligent and efficient solution for future smart transportation systems [14].

II. BACKGROUND & RELATED WORK

Accurate and timely traffic flow prediction (TFP) is a fundamental gateway to Intelligent Transportation Systems (ITS), and is fundamental for alleviating traffic congestion, facilitating urbanization, and improving transportation efficiency for smart cities[6]. By forecasting future traffic conditions, urban planners and traffic management centres can formulate land use policies, and infrastructure investments and make options for route guidance and direct traffic control [7].

A. *Traditional Traffic Prediction*

TFP methods have historically advanced from quite simple mathematical statistics and time series models like ARIMA

[5], to more complicated machine learning (ML) models. All of the earlier parametric methods like ARIMA, Vector Auto-Regressive (VAR)[4], and Kalman filters, sought to capture the temporal structure, but struggled with non-stationarity and non-linearity of the "real-life" traffic data[1]. Some of the early, non-parametric methods were able to better capture complicated, non-linear relationships with Support Vector Machines (SVM), K-Nearest Neighbours (KNN), and Artificial Neural Networks (ANN)[1].

ARIMA model formula (general form)

$$X_t = c + \sum_{i=1}^{p} \phi_i X_{t-i} + \sum_{j=1}^{q} \theta_j \varepsilon_{t-j} + \varepsilon_t \qquad (1)$$

Since the emergence of big data and with the increased compute capabilities, Deep Learning (DL) models have recently claimed the title to the "highest performance" TFP models, detecting complex spatio-temporal dependencies[5]. More developed models like Long Short-Term Memory (LSTM), Gated Recurrent Units (GRU) or combined models have been shown to effectively extract temporal features within the spatio-temporal data. To detect spatial relationships, as with most traffic networks which are delicate non-Euclidean graphs, Graph Neural Networks (GNN) have been important in TFP for networks; this includes Graph Convolutional Networks (GCN) and Graph Attention Networks (GAN) models. TFP models that combine both spatial and temporal modelling include:

- ST-GCN
- T-GCN
- ASTGCN
- DCRNN
- Graph-WaveNet

All of these combination methods, including the others listed throughout this chapter, have been shown to produce accurate predictions across a range of traffic applications [9][4][17].

However, these robust DL-based methods are usually described based on a centralized training paradigm that aggregates substantial amounts of rich traffic data from various distributed sources (e.g., sensors, organizations) into one centralized data centre/cloud[14]. This centralized paradigm presents a number of significant challenges, such as data sharing and inherent privacy risks. Traffic data and analytics, for instance, may include GPS locations, license plate numbers, and traveller trajectories which underpin sensitive information[8].

The further traffic data is centralized in a data centre, the larger the breach or misuse that could occur as a centralized data system entails sensitive datasets. With recent developments in data privacy laws, such as the European Union's General Data Protection Regulation (GDPR) and California Consumer Privacy [1] Act, the prospective collection, processing and sharing of personal data are strictly outlined, making a centralized data aggregation process both difficult and legally questionable[5]. The need for data sharing and consent around personal data involves considerable privacy issues and create substantial data silos in which different organizations cannot simply train robust models collaboratively and work with their respective distributed data expertise[8].

B. *Federated Learning Fundamentals*

Federated Learning has arisen as a useful distributed machine learning paradigm in light of the constraints of centralized training, especially around data privacy and the distributed nature of the data[7]. Federated learning was first introduced to the research community by Google in 2016 [2]] as a process where multiple entities (clients or organizations) can collaboratively train a model while keeping their raw training data private and not exchanging data witheach other orntralizing training data. According to FL, this follows the principle of "bringing the code to the data, not the data to the code" [11]. The general process of FL includes

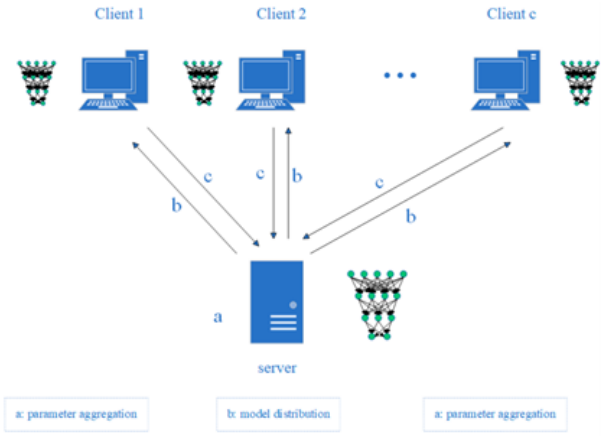


Fig. 3. Federated learning workflow. Source:This image is taken as reference from [7]

downloading the current global model for a client, training locally on a private data set, and sending only model updates or parameters back to the central server for aggregation [7]. The server aggregates model updates to create a new global global model to send back to the clients for the next round of training [18]. The most popular aggregation algorithm is Federated Averaging (FedAvg) [7], where the model parameters or gradients are averaged together that have been uploaded from the client's weightings for the client's averages are based on the relative sizes of their local training datasets [10]. This can be mathematically expressed as

$$w_{t+1} = \frac{1}{\sum_{k=1}^{K} n_k} \sum_{k=1}^{K} n_k w_{t+1}^{(k)} \qquad (2)$$

where $w_{t+1}^{(k)}$ is the model update from client k, and n_k is the number of data points on client k.

While FL implicitly safeguards data privacy by keeping raw data decentralized[7] , additional methods for enhancing privacy can be incorporated in FL. One method is known as differential privacy (DP). DP can be incorporated into FL by introducing noise into the model updates before they are sent to the server, resulting in some provable privacy

guarantees proposed a federated learning algorithm that incorporates differential privacy protections based on noise addition. Secure aggregation is another method that uses cryptographic approaches to ensure that only the aggregate update is learned by the server and will never see or have access to individual client updates[11] . A common form of applying differential privacy is by adding Laplace noise to the output of a function f on dataset

$$\mathcal{M}(D) = f(D) + \text{Laplace}\left(0, \frac{\Delta f}{\epsilon}\right)$$

Despite its advantages, FL faces several key challenges: Client datasets are often not independent and identically distributed (non-IID) . This heterogeneity could lead to local models diverging sufficiently from the global model to effectively bias the model that gets aggregated, which could degrade performance over centralised training [6] . This challenge is evident when client gradients diverge significantly from the global objective:

$$\nabla f(w) \neq \frac{1}{K}\sum_{k=1}^{K} \nabla f_k(w)$$

indicating that each client's update $f_k(w)$ may not align with the overall optimization direction [6] . For example, in TFP, traffic flow patterns vary based on geographical region and cause the resulting datasets among the devices or organizations, to be non-IID [13] .

Transmitting any model updates or parameters from clients to server will incur communication costs, with some deep learning models having many parameters causing substantial communication costs [8] . While FL can reduce the communication costs in comparison to sending centralized data, convergence can still require frequent communication rounds, so that the communication for the number of local epochs is largely dependent on the datasets being non-IID. Overload communication can lead to the increase in delay for collecting traffic flow information[7] .

C. FL in Traffic Prediction

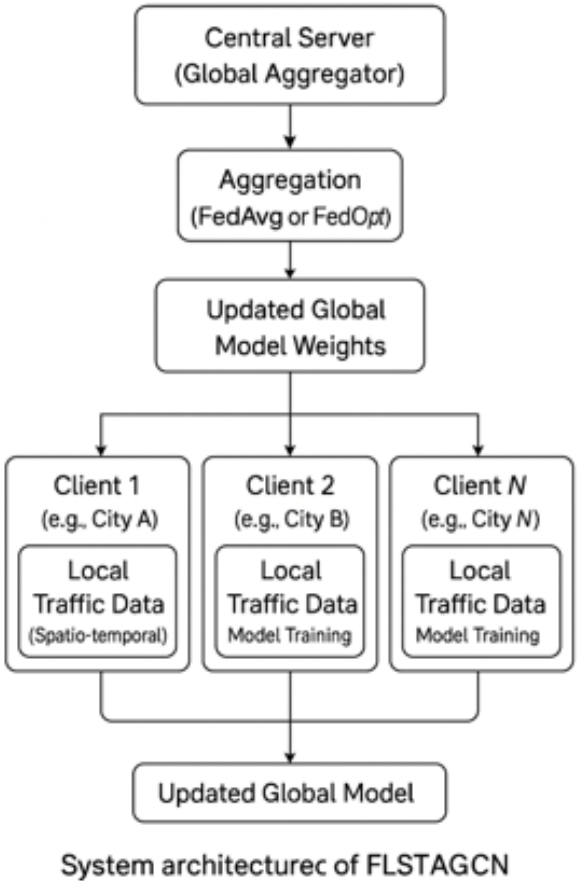
Considering its potential for training models on decentralized data without compromising privacy, federated learning (FL) continues to gain traction for use in traffic flow prediction. The decentralized characteristics of modern Intelligent Transportation Systems (ITS) with multiple sensors and organizations fits well with the approach of FL[7] , however, the use of FL to TFP is still considered very much in its infancy [14].

The research presented here considers the use of FL, focused on different FL architectures and methods, adapted to the spatio-temporal form of traffic data and to the still unclear environment of TFP.

*1) **FL Architectures** :* Different deep learning models are integrated into the FL framework for TFP

FLSTAGCN - Federated Learning with Spatial Temporal Attention Graph Convolutional Networks

Shi et al. proposed the FLSTAGCN, a Federated Learning-based Attention Graph Convolutional Network for TFP. This model combines the Spatial-Temporal Attention Graph Convolutional Network (STAGCN), which combines attention mechanisms to extract spatio-temporal features, with a FL framework that contains an optimal selection protocol for more efficient aggregation. The results showed that the FLSTAGCN can achieve prediction performance that is similar or slightly better than some centralized state-of-the-art methods (e.g. STFGNN), while ensuring data privacy [5].



System architecturec of FLSTAGCN

Fig. 4. System architecture of FLSTAGCN model.

PLFL - Personalized Lightweight Federated Learning

Personalization, Dealing with the non-IID characteristics of traffic data is essential, as no single global model may accurately represent the local traffic characteristics for each client location. Personalized Federated Learning (PFL) methods propose to adapt models to client preferences [18].

Dai et al. proposed a Personalized Lightweight Federated Learning (PLFL) framework for short-term TFP. PLFL maximizes communication efficiency through dynamic model pruning and enhances personalization through the awarding of weight customized for individualized client models based on data features of interest. The purpose of PLFL is to maintain the unique characteristics of each client's data [7].

BFRT - Blockchained Federated Real-time Traffic Prediction

Edge/Real-Time FL, Recent ITS need low-latency, real-

time predictions, able to adaptively address dynamic traffic conditions across many aspects of complex systems, such as unexpected nonrecurring events. Streaming FL methods are designed to continuously train a model, taking in newly arriving data [13].

Meese et al. introduced BFRT, a blockchained federated learning architecture for real-time TFP with real-time data and edge computing. BFRT, which was application of federated learning with a permissioned blockchain network, was able to use roadside units (RSUs) as edge devices. BFRT distinguished that streaming FL can provide lower real-time predictive error rates than each device using respectively trained centralised models [10].

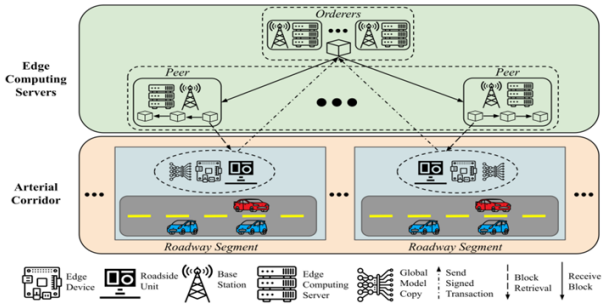


Fig. 5. System architecture of BFRT. Source: This image is taken as reference from [10].

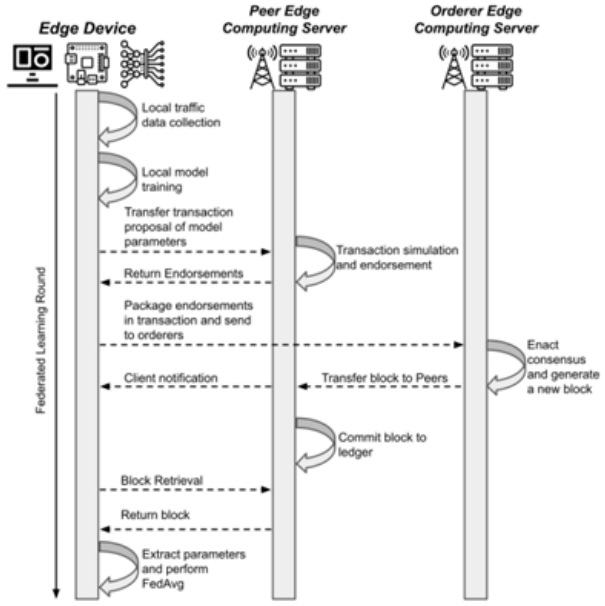


Fig. 6. Workflow of BFRT. Source: This image is taken as reference from [10].

FedTPS - Federated Traffic Prediction with Synthetic Data Augmentation

Orozco et al. presented FedTPS, a Federated Learning framework for Traffic Flow Prediction with Synthetic Data Augmentation. FedTPS addresses two issues impacting FL for traffic prediction: data heterogeneity, and data scarcity. FedTPS works in two stages by first, training a generative model federatively (TFDiff) that produces synthetic data capturing the global distribution, and second, training a federated traffic flow prediction model (either GATAU or any model proposed that works) based on the client data, but enhanced with synthetic data. This method shows improvement in the general model performance and robustness, especially when it is faced with non-IID data [17].

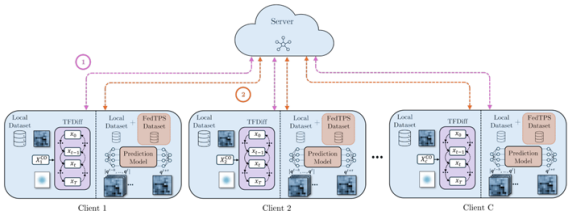


Fig. 7. Framework of BFRT. Source: This image is taken as reference from [17].

III. Comparative Analysis

Federated Learning (FL) has become a very effective and promising strategy for Traffic Flow Prediction (TFP) by permitting the collaborative model training of many data owners, such as organizations or traffic sensors, without them having to share their raw (and potentially privacy-sensitive) data [7]. With a decentralized approach, FL provides an innovative alternative to traditional centralized approaches (which often include centralizing and processing large and centralized amounts of data, with privacy and bandwidth issues) [18]. The objective of FL based TFP approaches is to keep or improve upon prediction accuracy along with dealing with important challenges related to distributed learning, mostly data heterogeneity and communication constraints [6].

Different approaches were proposed with different underlying model architectures and ways of solving the issues. Many of the approaches utilized spatio-temporal graph neural networks (GNNs) to model the intricate dependencies present in traffic data and incorporated these into FL frameworks[5]. Examples of such models include FedGRU, FCGCN (a GCN with community detection), FLSTAGCN (an attention-based GCN), FedSTN (which uses graph representation and semantic features), PFL-GTCN (combines TCN and GCN) and FedTFP (an attention-based spatio-temporal GCN called AFSTGCN) that utilize sophisticated models from deep learning in the context of FL. PLFL introduces a personalized lightweight federated learning paradigm using a spatiotemporal fusion GCN as the base model [6].

One essential issue in using FL in TFP is the heterogeneity of traffic data across clients, which can erode the performance of a single global model over all clients. Personalized Federated Learning (PFL) methods are designed to create models that meet the particular characteristics and needs of a client [7]. PLFL adds personalization by giving each client model specific weights based on client data features

and measuring the dissimilarity of the local and global model parameters when aggregating. PFL-GTCN aimed to create aggregation weights per client that would adjust due to the contribution of an individual client's data to the global model, an effort to reduce iterations and communication overhead, likewise. FedNe proposed a method of personalization that would exploit physical connectivity and similarities between client connected subgraphs to create personalized models [7]. When paired with dynamic model pruning in FedNe-DP, this approach looked to make it more feasible to work with heterogeneous graph-structured data [8]. FedTFP would address heterogeneity through various procedures, including segmenting the road network based on flow pattern similarities using DTW and K-means algorithms rather than geographic proximity alone, creating personalized and "meme" models for training locally, and using Deep Mutual Learning (DML) as knowledge distillation for bridging model and objective heterogeneity [9]. NeighborFL utilizes a personalized FL approach in which each device selects a group of peer local models dynamically, in addition to its own, to build its aggregated model by minimizing real-time prediction error. The group of models that each device uses in NeighborFL for aggregation can vary depending on distances, evaluation results, etc. This dynamic process contrasts with static grouping techniques [13]. FedTPS deals with data heterogeneity by training a federated generative model to generate synthetic traffic flow data and use this data to augment the local dataset of each client, so that client data will better describe the overall traffic flow distribution [17].

Another important consideration for any guild is the communication efficiency, since data inferred from potentially large model updates has to be communicated to the server through potentially large updates from many clients at once, which may not be trivial in a constrained environment [18]. There are many mechanisms that implement some method to reduce the potential cost of the communication. DPruneFL, the client's model pruning mechanism, introduced up to FedNe-DP, allows client-side model pruning to remove the non-personalized parameters which effectively decrease the number of parameters that need to upload to the server. As a result, only the non-pruned parameters would be communicated to the parameter server which significantly reduces the communication costs [18]. FedGRU is focused on the GRU model used for TFP, but they suggest a Joint-Announcement Protocol for implementing the largest expected gain for distributed FL, which randomly selects organizations that will participate in each training round. REFOL is a resource-efficient federated online active learning method which uses something called data-driven client participation, measures concept drift and determines if the client needs to participate in an update to the model, avoiding any communication and computational costs incurred from unnecessary participation. REFOL also added spatial correlation evaluation factors into the aggregation process such that it does not incur extra communication costs to the client [16].

Several FL techniques specifically support real-time or online learning in order to be able to adapt to the constantly changing traffic conditions and respond to concept drift [13]. For example, FedOSTC was introduced to support online spatio-temporal correlation-based FL, where each vehicle would utilize online gradient descent (OGD) that incrementally updates each local model on good time to reflect new data sources as they arrive. The authors proposed a period-aware aggregation mechanism which sought to improve the generalization of the global model based on periodic characteristics typically evident in traffic flow. In another venue, REFOL improved online learning by detecting concept drift through Kullback-Leibler Divergence (KLD), which gave clients the flexibility to choose between using existing models or updating their models in a way that maximized resources . Finally, NeighborFL included an error-driven aggregation process that lets devices build their personalized model components based on real-time prediction errors, following the lines of adaptive algorithms to adjust their predictions to rapidly change traffic dynamics[16].

Security and privacy are also fundamental features of FL. While the typical form of FL maintains privacy over data by keeping the raw data local and only sharing updates to the model, some methods offered additional or alternatively secure features [7]. B2SFL and BFRT use blockchain technology to allow for data integrity, traceability, system scalability, and possibly secure aggregation and data sharing [14]. B2SFL, specifically, is proud of its use of a Distributed Homomorphic-Encrypted Federated Averaging (DHFA) algorithm to secure computation used to aggregate parameters with the use of partial homomorphic encryption. FedSTN also refers to "simulating the use of a Paillier-based Additive Homomorphic Encryption (AHE) approach for secure parameter sharing," but, did not use it to prove secure parameter sharing took place. FedGRU did mention that it uses the PySyft framework to encrypt parameters within its implementation. Some methods also reference differential privacy in some form as a potential privacy enhancing technique[14].

TABLE II

COMPARISON OF PREDICTION PERFORMANCE OF DIFFERENT MODELS (RESULTS REPRESENT 5 MIN, 15 MIN, AND 30 MIN PREDICTION PERFORMANCE, RESPECTIVELY). THIS TABLE IS TAKEN AS REFERENCE FROM [7]

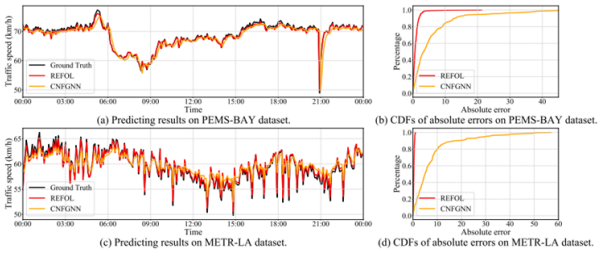
Model	RMSE	MAE
LSTM	9.12 / 10.09 / 11.63	6.23 / 6.97 / 7.95
TGCN	8.43 / 8.93 / 9.51	5.59 / 5.95 / 6.58
DCRNN	7.86 / 8.03 / 8.22	4.89 / 5.01 / 5.32
STGCN	7.57 / 7.88 / 8.09	4.55 / 4.82 / 5.16
PLFL	7.11 / 7.63 / 8.21	4.05 / 4.79 / 4.98

As evidenced by the experimental results found in the sources, the proposed FL-based TFP methods generally present significantly better performance than a variety of baselines, including traditional methods, and in some cases other FL methods. In Table 2,PLFL is reported to demonstrate significant superiority to LSTM, TGCN, DCRNN, and STGCN in prediction accuracy (RMSE and MAE) and short-

term predictions. It also showed superior performance to other common personalized FL methods such as FedTC, FedMCSA, and pFedKT although it was still relatively balanced across clients with differing data amounts. fedNe-DP is reported to show lower average MAE and RMSE relative to FedAvg, LotteryFL, FedPrune, and FedNe, suggesting relatively effective handling of the heterogeneous nature of graph data. NeighborFL has a lower average device MSE in the last 24 rounds, and for the entire simulation, than Centralized, NaiveFL, and r-NaiveFL approaches. FedOSTC is said to outperform centralized and other FL methods (CenterOff, CenterOn, FedAvgOff, FedAvgOn CNFGNN) in RMSE and MAE measures over two datasets. REFOL is claimed to outperform a number of centralized and FL baselines (including FedOSTC and CNFGNN) in RMSE and MAE across both datasets, with very significant reported gains. FedTFP claims very significant improvement, in MAE , RMSE, and MAPE over FCGCN and the DST-GCN baseline FL models, with FedTFP's success said to be due to a pattern similarity based road network division, DML for heterogeneity, and a multi-factor weighted aggregation strategy [7].

Methods	PEMS-BAY						METR-LA					
	5min ($F=1$)		30min ($F=6$)		1h ($F=12$)		5min ($F=1$)		30min ($F=6$)		1h ($F=12$)	
	RMSE	MAE	RMSE	MAE	RMSE	MAE	RMSE	MAE	RMSE	MAE	RMSE	MAE
SVR	2.01	1.09	3.74	1.79	4.80	2.28	6.43	3.46	8.41	4.34	9.61	5.00
GRU	2.02	0.99	3.93	1.77	5.50	2.42	5.56	**2.91**	8.13	4.17	9.41	4.90
DCRNN	1.65	0.93	4.79	2.09	6.19	2.71	4.30	3.57	7.09	4.61	8.71	5.33
STGCN	1.46	**0.86**	3.62	1.73	4.43	2.26	5.92	3.82	8.60	4.62	10.66	5.92
MegaCRN	1.61	0.91	4.42	1.94	5.33	2.33	4.24	3.54	6.77	4.51	8.11	5.09
FedAvg	1.80	1.02	3.72	1.78	5.25	2.41	5.84	3.32	8.16	4.45	9.52	5.22
FedGRU	1.82	0.97	4.72	2.27	6.52	3.37	5.71	2.99	9.23	5.00	11.03	6.56
FCGCN	9.25	4.82	9.45	4.97	9.36	5.04	15.37	9.69	15.45	10.04	15.16	9.83
FASTGNN	5.32	2.82	6.06	3.20	6.84	3.76	11.73	7.27	12.98	8.23	12.82	8.16
CNFGNN	1.82	1.04	3.60	1.73	5.13	2.64	5.82	3.25	8.03	4.24	9.38	5.12
FedGTP	1.75	1.00	4.59	2.06	6.10	2.74	6.11	2.96	9.34	4.40	11.77	5.66
pFedCTP	5.29	2.84	6.49	3.40	7.43	3.92	8.88	5.21	10.56	6.02	12.08	7.15
REFOL	**1.00**	1.00	**1.86**	**1.61**	**2.44**	**2.08**	**3.29**	3.29	**4.87**	**4.02**	**5.29**	**4.21**

Fig. 8. REFOL performance compared with CNFGNN on PEMS-BAY and METR-LA datasets. (a, c) Predicted traffic speed vs. ground truth. (b, d) CDFs of absolute errors, showing REFOL's lower error concentration. Source: This table is taken as reference from [16].



(a) Predicting results on PEMS-BAY dataset. (b) CDFs of absolute errors on PEMS-BAY dataset. (c) Predicting results on METR-LA dataset. (d) CDFs of absolute errors on METR-LA dataset.

Fig. 9. Ground truth values and forecasting values of CNFGNN and REFOL. Source: This photo is taken as reference from [16].

FL for TFP is still a popular research area, and further studies aim to promote and ultimately advance prediction accuracy, enhance communication and computation efficiency, improve robustness against heterogeneity and concept drift, and achieve stronger privacy assurances. The further work described appears to include external factors, such as incorporating weather, improving aggregation algorithms, dealing with asynchronous FL settings, predicting non-recurrent events, allowing predictions across multi-cities, and finding more seamless ways to include privacy-preserving techniques [7].

IV. Future Directions

Federated Learning (FL) provides a robust framework for traffic flow prediction (TFP) with multiple organizations able to train models without the need to exchange raw data[7]. In addition, FL is practically advantageous, given the potential privacy implications and unique decentralized issues of traffic data [5].

The application of FL in TFP has challenges, such as data heterogeneity, where traffic and data distributions can vary widely among clients and locations, and communication overhead, which involves the transfer of potentially very large model parameters between clients and the centralized server.

One way to address data heterogeneity is through personalized federated learning (PFL) methods, which often utilize aggregation weights that examine the difference between the characteristics of the client data, the characteristics of the models, or by the relative importance of the clients' data, potentially with an attention mechanism approach. Neighbor-based aggregation (using neighbor, or relationships, or similarities between clients) is one way to personalize and promote knowledge transfer [8].

Communication efficiency is highlighted in its ability to incorporate mechanisms such as dynamic model pruning, in which the importance of parameters within localized models is determined and then purged prior to communications, as well as client selection protocols [7] [5].

Traffic environments are dynamic and constantly evolving, therefore models will need to adjust continuously and incorporate the concept drift. Models in Federated Online Learning (FOL) and other similar real-time adaptation approaches will promote continuous learning and at times even use data-driven approaches to inform the use of localized model updates [10].

These models within FL environments use advanced deep learning architectures, most commonly spatio-temporal graph convolutional neural networks (GCNs) and RNNs, such as LSTMs (Long Short-term Memory) and GRUs (Gated Recurrent State), very often augmented with additional attention mechanisms [4]. Localized models may even include external features such as points of interest (POI) and weather details. Data sparsity and heterogeneity may be countered through an enhancement in the generation of synthetic data by utilizing generative models during the FL development process [17]. Model and objective heterogeneity may require deep mutual learning or weight factor aggregation [9].

FL alone already resulted in some established protection of inherent raw data privacy, but the incorporation of additional real-time security measures and transparency may have an even wider range of benefits, bringing in blockchain technology for secure aggregation and auditing, or using some forms of homomorphic encryption that perform computations of encrypted data [14].

V. CONCLUSIONS

Federated Learning (FL) represents a new paradigm in privacy-preserving, decentralized machine learning unlike steady-state data analysis for training a model on a single device, FL learning is dynamic and is an ideal approach for the barriers faced in traffic flow prediction (TFP) in intelligent transportation systems. In this review, we examined a variety of FL-based TFP methods that utilized deep spatio-temporal models, with GRUs, GCNs, and attention mechanisms. The forms of the FLSTAGCN, FedNe, and PLFL have highlighted accurate predictive results and have started to address various barriers: non-IID data, communication efficiency, personalization. Despite the advancements, these works still had limitations. Many models do not perform well in the presence of concept drift, which is common in dynamic traffic conditions. Many do not have an optimal solution to communication issues in large scale deployments. Furthermore, there are no standardized benchmarks and datasets that can be used to ensure some level of consistent assessment across methods.

Future research should be invested in focus on cross-domain transferability, seamless online learning, and structured integration of external contextual information (e.g., weather forecasts, local events, etc.). We believe that personalized Federated Learning (FL), as well as synthetic data augmentation, represent especially promising future directions. As Federated Learning systems continue to mature, there will be a necessity to engage with real-world challenges (edge-device limitations, data heterogeneity) that have important implications for how models are designed ultimately to have any meaningful impact in practice. FL is not just a theoretical solution, but a framework for collaborative intelligence. The application of FL to traffic systems contributes to better predictive prospect and encourages ethical and privacy conscientious innovation in smart city infrastructure.

ACKNOWLEDGMENT

I would like to express my gratitude towards Ms. Anna-Lena Schlamp for providing her valuable insights and guidance throughout the process, correcting our mistakes and explaining every minor thing in detail. I sincerely thank her for putting her time and effort and giving her constructive feedback, which significantly enhanced the quality of this paper. This work would not have happened without her support and leadership.

REFERENCES

[1] Y. Liu, J. Yu, J. Kang, D. Niyato, and S. Zhang, "Privacy-Preserving Traffic Flow Prediction: A Federated Learning Approach," *IEEE Internet of Things Journal*, 2020.

[2] M. Xia, D. Jin, and J. Chen, "Short-Term Traffic Flow Prediction Based on Graph Convolutional Networks and Federated Learning," *IEEE Trans. Intell. Transp. Syst.*, 2023.

[3] M. Yaqub, S. Ahmad, M. Manan, and I. Chuhan, "Predicting Traffic Flow with Federated Learning and Graph Neural with Asynchronous Computations Network," *arXiv preprint arXiv:2401.12345*, 2024.

[4] X. Yuan, J. Chen, J. Yang, N. Zhang, T. Yang, T. Han, and A. Taherkordi, "FedSTN: Graph Representation Driven Federated Learning for Edge Computing Enabled Urban Traffic Flow Prediction," *IEEE Trans. Intell. Transp. Syst.*, 2023.

[5] L. Shi et al., "FLSTAGCN: Traffic Flow Prediction Based on Federated Learning and Attention Graph Convolutional Network," *Proc. IEEE Int. Conf. Systems, Man and Cybernetics*, 2024.

[6] T. Liu, Y. Wang, H. Zhou, J. Luo, and F. Deng, "Distributed Short-Term Traffic Flow Prediction Based on Integrating Federated Learning and TCN," *IEEE Access*, 2024.

[7] G. Bo and J. Tang, "A Short-Term Traffic Flow Prediction Method Based on Personalized Lightweight Federated Learning," *Italian Nat. Conf. on Sensors*, 2025.

[8] J. Guo, X. Feng, and H. Zheng, "Personalized Federated Learning with Neighbor Aggregation for Traffic Flow Prediction," *Int. Conf. Innovative Computing and Cloud Computing*, 2023.

[9] J. Feng, C. Du, and Q. Mu, "Traffic Flow Prediction Based on Federated Learning and Spatio-Temporal Graph Neural Networks," *ISPRS Int. J. Geo Inf.*, 2024.

[10] C. Meese, H. Chen, S. Asif, W. Li, C. Shen, and M. Nejad, "BFRT: Blockchained Federated Learning for Real-time Traffic Flow Prediction," *Proc. IEEE/ACM Int. Symp. Cluster, Cloud and Internet Computing*, 2022.

[11] K. Bonawitz et al., "Towards Federated Learning at Scale: System Design," *Proc. USENIX Workshop on Tackling Computer Systems Problems with Machine Learning*, 2019.

[12] H. Alnami and M. Mohzary, "VehiCast: Real-Time Highway Traffic Incident Forecasting System Using Federated Learning and Vehicular Ad Hoc Network," *Electronics*, 2025.

[13] H. Chen, C. Meese, M. Nejad, and C. Shen, "Individualized Federated Learning for Traffic Prediction with Error Driven Aggregation," *arXiv preprint arXiv:2404.01234*, 2024.

[14] H. Guo, C. Meese, W. Li, C. Shen, and M. Nejad, "B2SFL: A Bi-Level Blockchained Architecture for Secure Federated Learning-Based Traffic Prediction," *IEEE Trans. Services Comput.*, 2023.

[15] Q. Liu, S. Sun, M. Liu, Y. Wang, and B. Gao, "Online Spatio-Temporal Correlation-Based Federated Learning for Traffic Flow Forecasting," *IEEE Trans. Intell. Transp. Syst.*, 2023.

[16] Q. Liu et al., "REFOL: Resource-Efficient Federated Online Learning for Traffic Flow Forecasting," *IEEE Trans. Intell. Transp. Syst.*, 2024.

[17] F. Orozco, P. de Gusmao, H. Wen, J. Wahlström, and M. Luo, "Federated Learning for Traffic Flow Prediction with Synthetic Data Augmentation," *arXiv preprint arXiv:2403.56789*, 2024.

[18] H. Lai, J. Guo, X. Feng, and H. Zheng, "Communication-Efficient Personalized Federated Learning for Traffic Flow Prediction," *Int. Conf. Innovative Computing and Cloud Computing*, 2024.