Privacy-Preserving Aggregation for Federated Learning-Based Navigation in Vehicular Fog

Qinglei Kong, Feng Yin, Rongxing Lu, *Fellow, IEEE,* Beibei Li*, Xiaohong Wang, Shuguang Cui, *Fellow, IEEE* and Ping Zhang, *Fellow, IEEE*

***Abstract*—Federated learning-based automotive navigation has recently received considerable attention, as it can potentially address the issue of weak global positioning system (GPS) signals under severe blockages, such as in downtowns and tunnels. Specifically, the data-driven navigation framework combines the position estimation offered by the high-sampling inertial measurement units (IMUs) and the position calibration provided by the low-sampling GPS signals. Despite its promise, the privacy preservation and flexibility of the participating users in the federated learning process are still problematic. To address these challenges, in this paper, we propose an efficient, flexible, and privacy-preserving model aggregation scheme under a federated learning-based navigation framework named *FedLoc*. Specifically, our proposed scheme efficiently protects the locally trained model updates, flexibly supports the fluctuation of participants, and is robust against unregistered malicious users by exploiting a homomorphic threshold cryptosystem, together with the bounded Laplace mechanism and the skip list. We perform a detailed security analysis to demonstrate the security properties in terms of privacy preservation and dishonest user detection. In addition, we evaluate and compare the computational efficiency with two traditional schemes, and the simulation results show that our scheme greatly improves the computational efficiency during participant fluctuation. To validate the effectiveness of our scheme, we also show that only part of the model update is excluded from aggregation in the case of a dishonest user.**

***Index Terms*—Federated Learning, Privacy Preservation, Vehicular Fog, Vehicular IoT**

I. Introduction

The vehicular IoT has enabled better travel safety and onboard experience, which leads us toward a future of intelligent and autonomous transportation. Typical applications include predictive automotive maintenance [1], vehicle telematics [2], driver assistance, and autonomous vehicles [3]. Specifically, an accurate and reliable navigation model is built with the data collected by the high-sampling inertial measurement units (IMUs) in [4], which addresses the signal outage problem in a global navigation satellite system (GNSS). However, location-dependent vehicular IoT data are dispersively collected and maintained, and it could be difficult to centralize and manage them from the perspective of positions. To address this challenge, first, the vehicular fog architecture is proposed to push intelligence toward the network edge [5], in which the upgraded roadside units (RSUs) or cellular base stations act as fog nodes and make area-level decisions [6]. In this context, regional navigation models can be built distributively and operated with the collaboration of fog nodes and users. Second, the federated learning technique is also applied in data-driven navigation [4], which exploits the data gathered by mobile users and their onboard computation capabilities. However, to reach the full potential of vehicular IoT-driven navigation, several challenges remain to be addressed.

The foremost challenge is privacy preservation. Even though federated learning is intuitively viewed as a secure training method without centralizing raw data, studies have shown that model hyperparameters may still cause data leakage [7]. Secure aggregation mechanisms were proposed in [7], [8], which derive the aggregation results without the disclosure of each user's model hyperparameter. To achieve secure model aggregation, Bonawitz *et al.* [8] proposed a privacy-preserving scheme with the secure multiparty computation technique. However, the proposed scheme requires the transmission of public keys and the execution of mutual key agreements among all the users, which may not be applicable in the vehicular IoT scenario with intermittent connections. For example, when the vehicle-to-infrastructure (V2I) transmission during high-mobility handover is unstable, or when the vehicle-to-vehicle (V2V) transmission is out-of-coverage. Furthermore, the differential privacy technique has been integrated into secure aggregation schemes [9], [10]. Chase *et al.* [9] combined differential privacy with secure multiparty computation, where the differential privacy technique handles the privacy protection of the stochastic gradient descents, and the secure multiparty computation technique addresses the issue of collaboration. In addition, Truex *et al.* [11] further combined homomorphic encryption, secret sharing, and differential privacy to develop a protocol to balance privacy protection and model accuracy. As the scale of a model hyperparameter is immense, the intensive exploitation of computationally demanding homomorphic cryptographic operations may bring heavy computational complexity. Therefore, it is necessary to design an efficient and privacy-preserving model aggregation

Q. Kong is with Future Network of Intelligence Institute (FNii), the Chinese University of Hong Kong, Shenzhen, China 518172, and with the University of Science and Technology of China, China, e-mail: kongqinglei@cuhk.edu.cn.

F. Yin and S. Cui are with Future Network of Intelligence Institute (FNii), the Chinese University of Hong Kong, and the Shenzhen Research Institute of Big Data, Shenzhen, China 518172, e-mail: yinfeng@cuhk.edu.cn, and shuguangcui@cuhk.edu.cn.

R. Lu is with the Faculty of Computer Science, University of New Brunswick, Fredericton, Canada E3B 5A3, e-mail: rlu1@unb.ca.

B. Li is with the School of Cyber Science and Engineering, Sichuan University, Chengdu, China 610065, e-mail: libeibei@scu.edu.cn.

X. Wang is with the Institute for Infocomm Research (I2R), Agency for Science, Technology and Research (A*STAR), Singapore 138632, e-mail: wangx1@i2r.a-star.edu.sg.

P. Zhang is with State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing, China, email: pzhang@bupt.edu.cn.

*Corresponding Author: Beibei Li

scheme for federated learning-based vehicle navigation in vehicular fog.

The second challenge is the flexibility of participants. The users in vehicular IoT-based federated learning have only intermittent network connections and limited power supply, and mobile users may not be able to persist in the iterative training process from beginning to end. Although the secure aggregation schemes proposed in [8], [10] support user dropout, they fail to allow the participation of newcomers, which wastes the scarce sensory data collected by the newly arrived users. Moreover, once the user dropout occurs, the key reconstruction process may affect all users. However, changes in participants are frequent in vehicular fog. If a change to one participant causes the key reconstruction of all participants, heavy computation and communication overheads could be incurred. Therefore, there is also a need for an efficient and flexible model aggregation mechanism that supports user joining and leaving and is robust to dishonest users.

In this paper, to address these challenges, we propose a new flexible privacy-preserving model aggregation scheme under a federated learning-based navigation application in vehicular fog. The proposed scheme is characterized by supporting the flexible joining and leaving of participants and balancing the trade-off between computational complexity and privacy protection. Specifically, the contributions of this paper are threefold, as follows.

• First, we propose an efficient and privacy-preserving model aggregation scheme for federated learning-based navigation in vehicular fog, which balances the trade-off between computational complexity and privacy protection. Specifically, the proposed mechanism innovatively exploits a homomorphic threshold cryptosystem for key establishments and updates. It also utilizes the bounded Laplace mechanism [12] for the protection of model hyperparameters.

• Second, we provide a detailed analysis to show that our proposed scheme supports the flexible joining and leaving of participants. To be more specific, our scheme innovatively exploits a skip list for group division, and only the group members are required for a new round of key establishment during the participant fluctuation. The proposed scheme is robust to dishonest users through the authentication of the key aggregation result, and only the model hyperparameters in the detected group are excluded from model aggregation in the case of a dishonest user.

• Third, we demonstrate the security properties of our scheme in terms of privacy preservation and robustness to dishonest users. We show the effectiveness of the proposed scheme in the context of supporting dynamic user joining/leaving and then compare our scheme with two traditional schemes. We illustrate the robustness of the scheme against dishonest users and evaluate the trade-off between the privacy level and computational complexity.

The remainder of this paper is organized as follows. We introduce our system model, present our security requirements, and describe our design goals in Section II. In Section III, we present our efficient, flexible, and privacy-preserving model aggregation scheme for federated learning-based navigation. The security analysis and performance evaluations are performed in Section IV and Section V, respectively. Related work is described in Section VI. Finally, we conclude the paper in Section VII.

II. System Model, Security Requirements, and Design Goals

In this section, we describe the system model and identify the security requirements with the design goals.

A. System Model

We exploit the federated learning-based vehicle navigation framework *FedLoc* proposed in [4] as the basis of the system model under consideration (shown in Fig. 1). Specifically, the system utilizes the vehicular IoT data collected from IMU and global positioning system (GPS) to construct a neural network (NN)-based navigation model. Our scheme focuses on the interaction between a fog server and a group of users. Specifically, the proposed system has three types of entities:

- *Model Owner.* The model owner connects to multiple fog servers, and each fog server keeps a regional model for localized navigation. During the training initialization phase, the model owner identifies the spatial-temporal requirement of the learning task. Then, it delegates the training task to the covering fog server. The model owner transmits the model to be updated $M^{(0)}$ to the fog server, and it remains offline. At the end of the training process, the model owner receives the updated model $M^{(T)}$ from the fog server.
- *Fog server.* The fog server, such as an upgraded RSU or a cellular base station positioned near the network edge, is responsible for updating a regional automotive navigation model via T training iterations. At the beginning of iteration t, the fog server broadcasts the model $M^{(t-1)}$, as shown in Fig. 1. At the end of training iteration t, the fog server aggregates all model hyperparameters and derives $M^{(t)}$.
- *Users.* Each user (in the form of either a smartphone or vehicle) gathers IMU and GPS data and keeps the collected data in its local storage. For the navigation model, the input data $\boldsymbol{x}$ are derived from three types of IMU motion sensors—a linear acceleration sensor, rotation vector sensor, and gyroscope sensor—while the data $\hat{\boldsymbol{y}}$ collected from the GPS unit—the velocity and yaw angle—are exploited to calibrate the estimated or predicted output. At iteration t, a user with identity x_i computes the local model update $M_i^{(t)}$ using stochastic gradient descent on its local dataset with an NN.

Communication Model. The connections between the users and fog server are realized through the IEEE 802.11p Wireless Access for Vehicular Environment (WAVE) standard (a short- to medium-range communication technology operating at the 5.9 GHz band) [13]. The connection between the fog server and the model owner occurs through secure wired links with high bandwidth and low transmission delay, and it is assumed to be securely protected by the HTTPS protocol [14].

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TII.2021.3075683, IEEE Transactions on Industrial Informatics

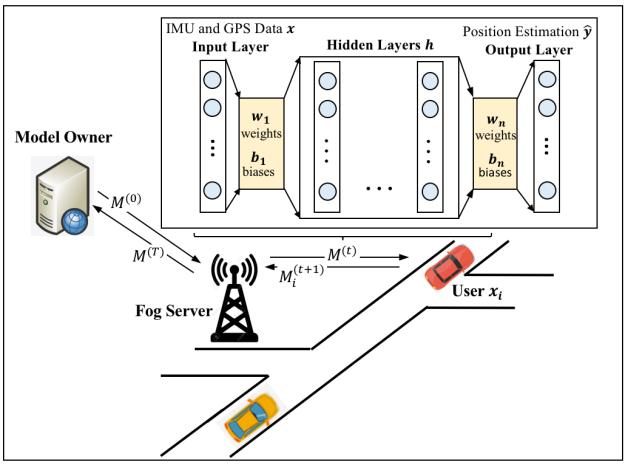


Fig. 1. Proposed federated learning-based navigation framework

B. Security Requirement

In the security model, we consider the fog server to be honest-but-curious; i.e., it will follow the defined protocol but is curious about each user's model hyperparameter. In our proposed scheme, we assume that all users register to the trusted authority (TA). However, only some users will register to the model owner, and some dishonest unregistered users will attempt to join and corrupt the learning process. Furthermore, we assume there is no collusion between any two entities, and all the registered users will honestly participate in the learning process. Specifically, the proposed scheme should satisfy the security requirements of privacy preservation and dishonest user detection.

- *Privacy Preservation.* During each training iteration, the fog server should not learn the content of each model hyperparameter. Meanwhile, each model hyperparameter should be hidden within at least a predefined threshold number of users.
- *Dishonest User Detection.* Users who are unregistered to the model owner but intend to join in the learning process are taken as dishonest users, who may present fake secret shares (in terms of random integers) to corrupt the learning process. The fog server should be able to detect cheaters and exclude them from the learning process.

C. Design Goals

With the above system model and security requirements, the goal is to design a privacy-preserving and flexible model aggregation scheme for federated learning-based navigation in vehicular fog.

The proposed scheme should meet the above security requirements. If the proposed scheme does not satisfy the security requirements, the privacy of the involved users may be violated, the users may not be willing to participate in the learning process, and the regional navigation models may not be correctly constructed.

The proposed scheme should achieve the goal of flexibility. As the federated learning framework supports the flexible joining and leaving of participants, the proposed privacy-preserving model aggregation mechanism should also be adaptive to this situation. Since unregistered dishonest users may corrupt the training process, the proposed scheme should resist such attacks.

The proposed scheme should achieve the trade-off between privacy preservation and efficiency. Since the scale of an NN is large, encrypting all model hyperparameters could impose heavy cryptographic operations. To reduce the computational complexity, we should evaluate the exploitation of computationally heavy cryptographic operations. We also should analyze the trade-off between privacy protection and computational efficiency.

III. Proposed Scheme

In this section, we propose a privacy-preserving model aggregation scheme for federated learning-based navigation in vehicular fog. Meanwhile, it supports participant fluctuation and is robust to dishonest users. Also, a homomorphic threshold cryptosystem based on the linear assumption [15], the bounded Laplace mechanism [12], and the skip list structure [16] lays the foundation for the proposed scheme.

A. System Initialization

We assume that a trusted authority (TA)—i.e., a traffic management authority—will bootstrap the entire system. Given the security parameter κ, the TA generates the bilinear parameters $(p, \mathbb{G}, \mathbb{G}_T, e, g)$, where $|p| = \kappa, g \in \mathbb{G}$ and $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$; for details of the bilinear pairing, refer to [17]. The TA selects a random number $sk = s \in \mathbb{Z}_p$ as the private key and computes the system public key $pk = g^s$. In addition, the TA publishes the system parameters: $params = (p, \mathbb{G}, \mathbb{G}_T, e, g, pk)$. During the registration of a user with identity $x_i \in \mathbb{Z}_p$, the TA computes and securely transmits the identity-based secret key $sk_i = g^{\frac{1}{s+x_i}}$ toward it.

During the initialization of a model owner with identity ID_c, the owner selects $w + 1$ random secret numbers $(\alpha_1, ..., \alpha_{w-1}, \beta, x_r) \in \mathbb{Z}_p^{w+1}$ and then computes $(g^{x_r}, e(g, g)^{\beta \cdot x_r})$. If user x_i is allowed to register with model owner ID_c, the owner selects a new random number $s_i \in \mathbb{Z}_p$, computes the secret share $(s_{i,1}, s_{i,2})$, and securely delivers $(s_{i,1}, s_{i,2})$ to user x_i, which is

$$\begin{cases} s_{i,1} = g^{\sum_{j=1}^{w-1} \alpha_j \cdot (x_i)^j + \beta + s_i}, \\ s_{i,2} = e(g^{x_r}, g^{s_i}). \end{cases} \tag{1}$$

During the initialization of a fog server with identity id_f, the server selects two random numbers $\mathcal{SK}_f = (u, v) \in \mathbb{Z}_p^2$ as secret keys, and then it computes and announces the public keys $\mathcal{PK}_f = (g_1 = g^{1/u}, g_2 = g^{1/v})$.

Remark 1: In our proposed scheme, all involved users register with the TA, but only a portion of users register with the model owner. Besides, we take a dishonest user as someone not being registered with the model owner but responds to a training task.

B. Training Task Announcement

The model owner ID_c identifies the spatial-temporal requirement for vehicular IoT, and it delegates the training task to a nearby fog server id_f. The fog server id_f identifies a time slot length T_r; i.e., users should respond to join the task announced within time period T_r. Besides, the fog server id_f announces a training task to all users with the following steps.

Step 1: If a user satisfies the training requirement and intends to join the task, it sends identity x_i to the fog server id_f and waits for its response. After time period T_r, the fog server id_f assigns a response sequence i to user x_i and formulates a user set $\mathcal{U} = \{(1, x_1), (2, x_2), ..., (n, x_n)\}$ with n users. If it meets the requirement that $n > w$, the fog server id_f broadcasts the user set $\mathcal{U}$.

Algorithm 1 Initialization

```
MaxLevel = 1; NumNode = 0;
for i = 1 to MaxLevel do
    header → forward[i] = header;
end for
```

Algorithm 2 Update(list, NumNode, Threshold)

```
newLevel = list → level+1; list → level = newLevel;
local update[1,...,list → level]
y = (list → level = 1) → header; IntUser = 0;
for i = 1 to NumNode do
    y = y → forward[1]; IntUser := IntUser+1;
    if (IntUser mod Threshold == 1 and IntUser <= NumNode-Threshold) or (IntUser == NumNode-Threshold+1) then
        z = (list → level = MaxLevel) → header
        for i = list → MaxLevel downto 1 do
            while z → forward[i] → key < y do
                z = z → forward[i];
            end while
            update[i] = z;
            y → forward[i] = update[i] → forward[i];
            update[i] → forward[i] = y;
        end for
    end if
end for
v = (list → level = MaxLevel) → header;
IntGroup = 0;
for j = 1 to ⌈n/w⌉ do
    IntGroup := IntGroup +1;
    v = v → forward[list → level = MaxLevel];
    U[IntGroup] = ∅; int = 0;
    while int < Threshold do
        int:=int+1; v_1 = v → forward[1];
        U[IntGroup] = U[IntGroup] ∪ v_1;
    end while
end for
```

Step 2: The fog server and the user set $\mathcal{U}$ first synchronously initialize a skip list with **Alg. 1**, and then they synchronously add members to set $\mathcal{U}$ with the *insert* and *update* operations. The *update* operation is shown in **Alg. 2**, and more details about the *insert* and *delete* operations in a skip list can be found in [16]. Fig. 2(a) shows an example of a skip list with user set size $|\mathcal{U}| = 8$ and threshold $w = 3$. If a new user $(9, x_9)$ intends to join in the learning process, the joining process is illustrated in Fig. 2(b). Fig. 2(c) shows what happens when user $(4, x_4)$ leaves the training process.

Note that we exploit the skip list to improve the efficiency during user joining and dropout. For example, when a new user $(9, x_9)$ enters the training process, only the members in Group u_3 are affected, as shown in Fig 2(b). On the other hand, when user $(4, x_4)$ leaves the training process (as shown in Fig. 2(c)), only members in the newly formulated Group u_2 are affected. Thus, our scheme reduces the computational complexity introduced by user joining and dropout.

C. Ciphertext Generation

After the group formulation process, we further discuss the ciphertext generation process. *Step 1:* If user x_i (for example, user x_2 in Fig. 2(a)) appears in only one group U_k (group U_1 in Fig. 2(a)), the user first chooses two random numbers $(r_i, r_i^{'}) \in \mathbb{Z}_p$ and then selects two random values $(k_i, k_i^{'}) \in \{0, 1, ..., \lfloor \frac{M}{w_{max}} \rfloor\}$, where w_{max} is the maximum allowable number of users in the training process. User x_i also selects two random numbers $(t_{i,1}, t_{i,2}) \in \mathbb{Z}_p^2$ and generates the ciphertext as follows:

$$\begin{cases} c_{i,1} = {g_1}^{t_{i,1}}, \\ c_{i,2} = {g_2}^{t_{i,2}}, \\ c_{i,3} = s_{i,1} \cdot g^{r_i/A_i} \cdot g^{-(t_{i,1}+t_{i,2})/A_i}, \\ c_{i,4} = (s_{i,2})^{A_i} \cdot e(g^{x_r}, g^{r_i}) \cdot e(g_1, g_2)^{k_i}, \\ c_{i,5} = s_{i,1} \cdot g^{r_i^{'}/A_i} \cdot g^{-(t_{i,1}+t_{i,2})/A_i}, \\ c_{i,6} = (s_{i,2})^{A_i} \cdot e(g^{x_r}, g^{r_i^{'}}) \cdot e(g_1, g_2)^{k_i^{'}}, \end{cases} \tag{2}$$

where $A_i = \sum_{j \in U_k, j \neq i} \frac{-x_j}{x_i - x_j} \mod p$. If a user exists in two groups (for example, id_6 exists in group U_2 and group U_3), the corresponding value A_i is derived as $A_i = \sum_{j \in U_k, j \neq i} \frac{-x_j}{x_i - x_j} + \sum_{l \in U_{k+1}, l \neq i} \frac{-x_l}{x_i - x_l} \mod p$. Note that our proposed scheme utilizes the homomorphic threshold cryptosystem based on the linear problem: to recover message $a \in M$, it suffices to compute the discrete logarithm of $e(g, g)^a$ with base $e(g, g)$ since $0 \leq a \leq M$, which takes only expected time $O(\sqrt{M})$ using Pollard's lambda method.

Step 2: User x_i selects another random number $\hat{r}_i \in \mathbb{Z}_p$ and generates the signature pair $(\sigma_{i,1}, \sigma_{i,2})$, which is

$$\begin{cases} \sigma_{i,1} = s k_i^{k_i^{'} + \hat{r}_i} = g^{\frac{k_i^{'} + \hat{r}_i}{x_i + s}}, \\ \sigma_{i,2} = e(g, g_1)^{\hat{r}_i}. \end{cases} \tag{3}$$

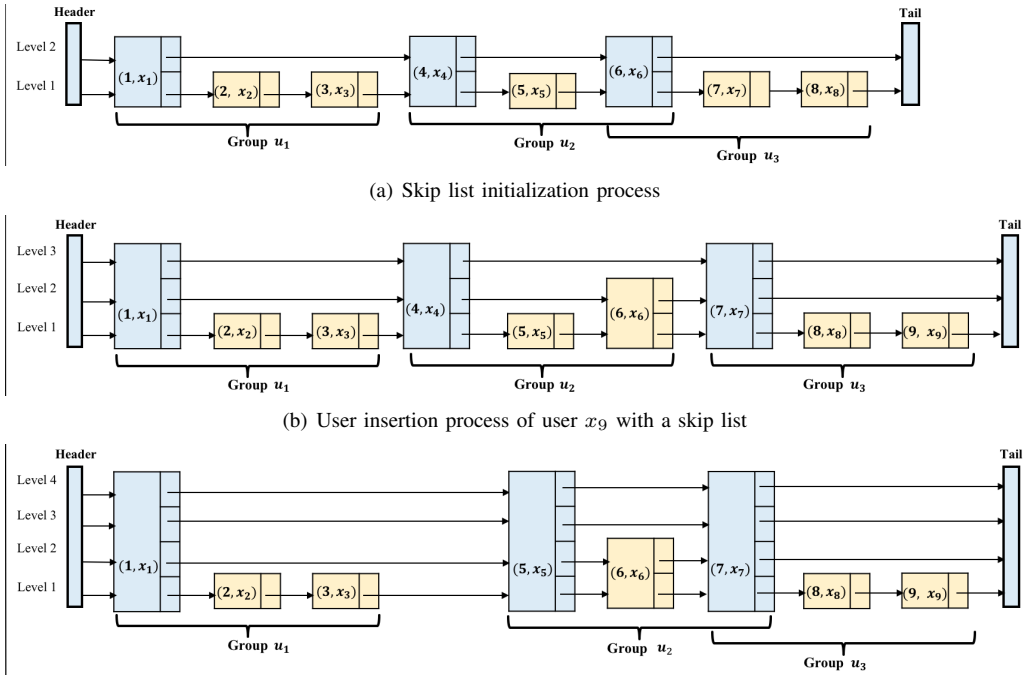
Step 3: For user x_i, the e-th dimension of the model hyperparameter $M_i^{(t)}$ is $m_{i,e}^{(t)}$, and the ciphertext is

$$d_{i,e}^{(t)} = H(id_f || e || t || TS) \cdot k_i + m_{i,e}^{(t)} + \eta_{i,e}^{(t)}, \tag{4}$$

where $\eta_{i,e}^{(t)}$ denotes the noise extracted from the bounded Laplace mechanism [12].

Step 4: User x_i organizes all ciphertexts $msg_i^{(t)} = x_i || t || c_{i,1} || c_{i,2} || c_{i,3} || c_{i,4} || c_{i,5} || c_{i,6} || \sigma_{i,1} || \sigma_{i,2} || d_{i,1}^{(t)} || ... || d_{i,l}^{(t)}$,

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TII.2021.3075683, IEEE Transactions on Industrial Informatics



(a) Skip list initialization process

(b) User insertion process of user x_9 with a skip list

(c) User deletion process of user x_4 with a skip list

Fig. 2. Example of a skip list initially with 8 users and 3 groups

where l is the dimension of model $M_i^{(t)}$. Then, user x_i securely sends $msg_i^{(t)}$ to fog server id_f.

Remark 2: The NN weights, which are commonly solved by minimizing the least-squares cost, provide a point estimate for a given dataset. To determine a proper value domain of the NN weights for our problem—i.e., the value range of the bounded Laplace mechanism—the bootstrap techniques in [18], [19] can be utilized to construct a confidence interval; for example, 95%, depending on our requirements. Fortunately, numerical evaluations of the two bounds can be performed offline without time and power constraints.

D. Ciphertext Aggregation

After receiving all messages $msg_i, i \in \mathcal{U}$, the fog server id_f performs the following steps.

Step 1: Fog server id_f aggregates the ciphertext $(c_{i,1}, c_{i,2}, c_{i,3}, c_{i,4}, c_{i,5}, c_{i,6}), i \in \mathcal{U}$ as follows:

$$\begin{cases} \hat{C}_1 = \prod_{i\in\mathcal{U}} c_{i,1} = g_1^{\sum_{i\in\mathcal{U}} t_{i,1}}, \\ \hat{C}_2 = \prod_{i\in\mathcal{U}} c_{i,2} = g_2^{\sum_{i\in\mathcal{U}} t_{i,2}}, \\ \hat{C}_3 = \prod_{i\in\mathcal{U}} (c_{i,3})^{A_i} = \prod_{i\in\mathcal{U}} s_{i,1}^{A_i} \cdot g^{\sum_{i\in\mathcal{U}} r_i - (t_{i,1}+t_{i,2})}, \\ \hat{C}_4 = \prod_{i\in\mathcal{U}} c_{i,4} = \prod_{i\in\mathcal{U}} s_{i,2}^{A_i} \cdot e(g^{x_r}, g)^{\sum_{i\in\mathcal{U}} r_i} \cdot e(g,g)^{\sum_{i\in\mathcal{U}} k_i}, \\ \hat{C}_5 = \prod_{i\in\mathcal{U}} (c_{i,5})^{A_i} = \prod_{i\in\mathcal{U}} s_{i,1}^{A_i} \cdot g^{\sum_{i\in\mathcal{U}} r_i' - (t_{i,1}+t_{i,2})}, \\ \hat{C}_6 = \prod_{i\in\mathcal{U}} c_{i,6} = \prod_{i\in\mathcal{U}} s_{i,2}^{A_i} \cdot e(g^{x_r}, g)^{\sum_{i\in\mathcal{U}} r_i'} \cdot e(g,g)^{\sum_{i\in\mathcal{U}} k_i'}. \end{cases} \tag{5}$$

Step 2: Fog server id_f derives the key aggregation result $\sum_{i\in\mathcal{U}} k_i$ with $\mathcal{SK}_f = (u, v)$, which is

$$e(g,g)^{\sum_{i\in\mathcal{U}} k_i} = \frac{\hat{C}_4}{e(\hat{C}_3 \cdot (\hat{C}_1)^u \cdot (\hat{C}_2)^v, g^{x_r})} \cdot e(g^{x_r}, g^{\beta})^m. \tag{6}$$

Correctness Analysis.

$$\begin{aligned} &\frac{\hat{C}_4}{e(\hat{C}_3 \cdot (\hat{C}_1)^u \cdot (\hat{C}_2)^v, g^{x_r})} \cdot e(g^{x_r}, g^{\beta})^m \\ &= \frac{\prod_{i\in\mathcal{U}} s_{i,2}^{A_i} \cdot e(g^{x_r}, g)^{\sum_{i\in\mathcal{U}} r_i} \cdot e(g,g)^{\sum_{i\in\mathcal{U}} k_i} \cdot e(g^{x_r}, g^{\beta})^m}{e(\prod_{i\in\mathcal{U}} s_{i,1}^{A_i} \cdot g^{\sum_{i\in\mathcal{U}} r_i - (t_{i,1}+t_{i,2})} \cdot (\hat{C}_1)^u \cdot (\hat{C}_2)^v, g^{x_r})} \\ &= \frac{\prod_{i\in\mathcal{U}} e(g^{x_r}, g^{s_i})^{A_i} \cdot e(g,g)^{\sum_{i\in\mathcal{U}} k_i} \cdot e(g^{x_r}, g^{\beta})^m}{e(\prod_{i\in\mathcal{U}} (g^{\sum_{j=1}^{w-1} \alpha_j \cdot (x_i)^j + \beta + s_i})^{A_i}, g^{x_r})} \\ &= \frac{\prod_{i\in\mathcal{U}} e(g^{x_r}, g^{s_i})^{A_i} \cdot e(g,g)^{\sum_{i\in\mathcal{U}} k_i} \cdot (g^{x_r}, g^{\beta})^m}{\prod_{i\in\mathcal{U}} e(g^{x_r}, g^{s_i})^{A_i} \cdot (g^{x_r}, g^{\beta})^m} \end{aligned} \tag{7}$$

Then the fog server id_f derives another key aggregation result $\sum_{i\in\mathcal{U}} k_i'$, which is

$$e(g,g)^{\sum_{i\in\mathcal{U}} k_i'} = \frac{\hat{C}_6}{e(\hat{C}_5 \cdot (\hat{C}_1)^u \cdot (\hat{C}_2)^v, g^{x_r})} \cdot e(g^{x_r}, g^{\beta})^m. \tag{8}$$

To detect dishonest users, fog server id_f authenticates the correctness of $\sum_{i\in\mathcal{U}} k_i'$ as follows:

$$e(\prod_{i\in\mathcal{U}} \sigma_{i,1}^{x_i}, g) \cdot e(\prod_{i\in\mathcal{U}} \sigma_{i,1}, g^s) \stackrel{?}{=} (\prod_{i\in\mathcal{U}} \sigma_{i,2})^u \cdot e(g,g)^{\sum_{i\in\mathcal{U}} k_i'}. \tag{9}$$

Step 3: Fog server id_f aggregates the ciphertexts and obtains

the aggregation result as follows:

$$\hat{d}_e^{(t)} = \sum_{i \in \mathcal{U}} H(id_f||e||t||TS) \cdot k_i + m_{i,e}^{(t)} + \eta_{i,e}^{(t)}. \quad (10)$$

Fog server id_f derives the model hyperparameter aggregation result in set $\mathcal{U}$, which is $\sum_{i \in \mathcal{U}} m_{i,e}^{(t)} + \eta_{i,e}^{(t)} = \hat{d}_e^{(t)} - \sum_{i \in \mathcal{U}} H(id_f||e||t||TS) \cdot k_i$.

IV. Security Analysis

In this section, we discuss the security properties of the proposed federated learning-based navigation scheme in vehicular fog.

• *The proposed model aggregation scheme is privacy preserving.* To construct a homomorphic threshold encryption scheme, we combine the Shamir secret sharing scheme with a homomorphic cryptosystem proposed in [15], where a secret share uploaded by each user is protected by the homomorphic cryptosystem proved to be secure under the linear decision assumption. If we take the item $s_{i,1}^{A_i} \cdot g^{r_i}$ as a message g^{m_i} of the ciphertext $(c_{i,1}, c_{i,2}, c_{i,3})$ in Eq. (2) is a ciphertext tuple of a homomorphic encryption cryptosystem based on a linear problem [15]. Based on another ciphertext pair $(S_{i,1}^{A_i} \cdot g^{r_i}, c_{i,4})$ protected by the secret share $(s_{i,1}, s_{i,2})$, the fog server cannot recover the individual key k_i and the aggregated key $\sum_{i \in \mathcal{U}} k_i$ can only be recovered with at least w users. Because the exploited homomorphic cryptosystem is shown to be semantically secure under the linear assumption [17], the aggregated ciphertext tuple $(\prod_{i \in \mathcal{U}} S_{i,1}^{A_i} \cdot g^{\sum_{i \in \mathcal{U}} r_i}, \prod_{i \in \mathcal{U}} c_{i,4})$ can be derived by the fog server with the secret key pair (u, v). Besides, the fog server can only recover the aggregated key $\sum_{i \in \mathcal{U}} k_i$, if it receives ciphertexts from more than w users.

Due to the large dimension of a model hyperparameter in an NN, we decide to reuse the user key k_i across multiple dimensions and iterations, as shown in Eq. (10). If the fog server derives both the upper and lower bounds of the message space, the fog server can recover the user key k_i, and this probability will be further discussed in Section V-C. In case k_i is inferred, we also exploit the bounded Laplace mechanism in [12] to protect $m_{i,e}^{(t)}$, such that its real value cannot be deduced even when $m_{i,e}^{(t)} + \eta_{i,e}^{(t)}$ is recovered.

• *The proposed model aggregation scheme is secure against dishonest users.* The secret share $(s_{j,1}, s_{j,2})$ of the dishonest user x_j is just two randomly chosen integers. We assume that user x_j encrypts value $k_j^{'}$ with $(s_{j,1}, s_{j,2})$, obtains the ciphertext $(c_{j,5}, c_{j,6})$ and then generates the signature pair $(\sigma_{j,1}, \sigma_{j,2})$ for $k_j^{'}$. Based on the ciphertext pair $(c_{j,5}, c_{j,6})$ generated by a dishonest user x_j, the fog server cannot correctly recover the aggregation result $\sum_{i \in \mathcal{U}} k_i^{'}$. Furthermore, the recovered aggregation result cannot be correctly verified via batch authentication, as shown in Eq. (10). The security of the identity-based signature that we exploit is shown to be secure under the *strong Diffie-Hellman (SDH) assumption* in groups with a bilinear map [17], and the aggregation result $\sum_{i \in \mathcal{U}} k_i^{'}$ cannot be correctly authenticated. Thus, the dishonest user can be detected through authentication.

V. Performance Evaluation

In this section, we evaluate the performance of the proposed scheme in vehicular fog. Note that the goal of our proposed scheme is to provide a privacy-preserving and flexible federated learning-based model aggregation scheme. We focus on showing the computational efficiency during user joining and dropout, robustness against malicious users, and the trade-off between privacy and complexity, which are highly relevant to privacy preservation. We show the effectiveness of our proposed scheme in terms of supporting the dynamic joining and dropout of participants and securing against dishonest users. We also investigate the trade-off between computational complexity and privacy protection. Specifically, we conduct experiments using a desktop with a dual-core processor Intel(R) Core(TM) i7-8700 CPU @ 3.20 GHz and 8.00 GB of installed RAM on a Windows 10 Enterprise platform.

To evaluate the performance of our scheme, we first compare it with another hybrid privacy-preserving federated learning model aggregation scheme, which was recently published in [11], and denote it as *traditional scheme 1*. To ensure a fair comparison with our proposed scheme, we make some changes to [11]. First, we assume that *traditional scheme 1* exploits the same homomorphic threshold encryption mechanism for protection. Second, instead of protecting model parameters with the computationally demanding homomorphic encryption technique, the model hyperparameters of each user are protected with a session key and the bounded Laplace mechanism. Similar to our proposed scheme, *traditional scheme 1* generally follows the same ciphertext generation steps defined in Section III-C. However, the main difference is that there is no group division, and the value A_i that appears in Eq. (2) contains all involved users in set $\mathcal{U}$, which is $A_i = \sum_{j \in \mathcal{U}, j \neq i} \frac{-x_j}{x_i - x_j} \mod p$.

In *traditional scheme 1*, whenever a user joins or leaves the training process, the entire session keys must be reconstructed. Specifically, when there is a member change in the user set $\mathcal{U}$, user x_i updates the value A_i in Eq. (2) for a new value $A_i^{'} = \sum_{j \in \mathcal{U}', j \neq i} \frac{-x_j}{x_i - x_j} \mod p$ with the updated user set $\mathcal{U}^{'}$. All members in set $\mathcal{U}^{'}$ generate the corresponding new ciphertext-tuples $(c_{i,1}, c_{i,2}, c_{i,3}, c_{i,4}), i \in \mathcal{U}^{'}$ and send the new ciphertexts toward the fog server. Furthermore, the fog server aggregates all received ciphertexts to obtain the aggregated value $(\hat{C}_1, \hat{C}_2, \hat{C}_3, \hat{C}_4)$ and further recovers the newly generated key aggregation result $\sum_{i \in \mathcal{U}'} k_i$.

We also compare our proposed scheme with another secure model aggregation scheme, which follows *protocol 4* proposed in [8] and denotes it as *traditional scheme 2*. Specifically, during the initialization phase, each user x_i generates and distributes its secret share β_i (in our scheme, there is only one secret share of the model owner β in Eq. 1), to all the potential users. We omit the key agreement process and retain only the process of secret sharing; refer to *protocol 4* proposed in [8] for more details. For the key establishment process, n pairs of ciphertexts $(c_{i,1}^t, c_{i,2}^t, c_{i,3}^t, c_{i,4}^t), i \in \mathcal{U}^{'}$ must be generated, and the fog server aggregates all ciphertexts for the value $(\hat{C}_1^t, \hat{C}_2^t, \hat{C}_3^t, \hat{C}_4^t)$. When a user joins/leaves the training process, as there is no group division of the users,

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TII.2021.3075683, IEEE Transactions on Industrial Informatics

user x_i also updates the value A_i in Eq. (2) into a new value $A_i^{'} = \sum_{j \in \mathcal{U}', j \neq i} \frac{-x_j}{x_i - x_j} \bmod p$.

A. Flexibility of User Joining and Leaving

Similar to the setup for traffic density estimation in [20], we assume that the fog server has a square coverage area of 1 km^2 and the traffic density varies from 100 to 2000 vehicles per hour. In addition, we set the length of each time slot to $ts = 1\ h$ and the probability of responding registered vehicles is 0.1. Thus, the vehicle scale ranges between 10 and 200. To determine the computational cost, we exploit the Java Pairing-Based Cryptography Library (JPBC) for bilinear parameters [21] and obtain the following computational costs: a single exponentiation operation in $\mathbb{G}$ is $C_e = 7.98$ ms, an exponentiation operation in $\mathbb{G}_T$ is $C_t = 0.57$ ms, and a bilinear pairing operation is $C_p = 4.49$ ms.

1) Computational Complexity Introduced by User Joining: In our proposed scheme, when a new user enters the training process, a new group with w users must be formulated. We consider only the key establishment process. To generate a ciphertext tuple $(c_{i,1}, c_{i,2}, c_{i,3}, c_{i,4})$ in Eq. (2), the introduced computational cost for all users is $w * (4 * C_e + 3 * C_t) + w * (C_e + 2 * C_t)$. For ciphertext aggregation and decryption, the introduced computational cost is $(w + 2) * C_e + C_p$. For *traditional scheme 1*, the introduced total computational cost for user joining is $n * (4 * C_e + 3 * C_t) + (n + 2) * C_e + C_p$. For *traditional scheme 2*, the introduced total computational cost is $n * (4 * C_e + (2 * n + 1) * C_t) + (n + 2) * C_e + C_p$. Furthermore, the comparison among the three schemes during the user joining process is shown in Fig. 3.

Fig. 3 shows the computational complexity of the user joining process concerning the number of users when the threshold is $w = 5$. Specifically, in our proposed scheme, the computational complexity of our scheme $O(w)$ increases to the number of users contained in each divided group. For *traditional scheme 1*, the computational complexity $O(n)$ increases with increasing scale of participants. *Traditional scheme 2*'s computational complexity $O(n^2)$ depends on the square of the user scale. Thus, in the context of user joining, only the users in the relevant group are influenced, which reduces the computationally demanding operations in the system.

2) Computational Complexity Introduced by User Dropout: In our proposed scheme, to reformulate a group after a user leaves, the user needs only to consume a computational cost of $4 * C_e + 3 * C_p$ to update $(c_{i,1}, c_{i,2}, c_{i,3}, c_{i,4})$. Unlike the user joining process, which only involves the users at the end of the skip list, the user leaving process may involve the group reformulation of multiple user groups in the skip list. In our proposed scheme, the expected computational complexity of the user leaving process is $((4 * C_e + 3 * C_p) * w + C_e * w) * (\lceil \frac{n}{w} \rceil + 1)/2 + 2 * C_e + C_p$. In *traditional scheme 1*, the corresponding computational complexity for a user leaving is $n * (4 * C_e + 3 * C_p) + (n + 2) * C_e + C_p$. For *traditional scheme 2*, the introduced total computational cost is $n * (4 * C_e + (2 * n + 1) * C_t) + (n + 2) * C_e + C_p$.

Fig. 4 shows the computational complexity of the user leaving process to the number of users when the threshold is set to $w = 5$, and the evaluation results show that our proposed scheme greatly reduces the computational complexity introduced by leaving. During the user leaving process, the computational complexity of our scheme $O(w * \lceil \frac{n}{w} \rceil)$ mainly depends on the number of users contained in each divided group. For *traditional scheme 1*, the computational complexity $O(n)$ is related to the scale of the participants. *Traditional scheme 2*'s computational complexity $O(n^2)$ depends on the square of the user scale. Thus, in the context of user joins, only the users in the relevant group are influenced in our scheme, which reduces computationally demanding operations. Therefore, in the context of a user leaving the training process, only the users in the newly formulated group are affected, which further reduces computationally demanding operations.

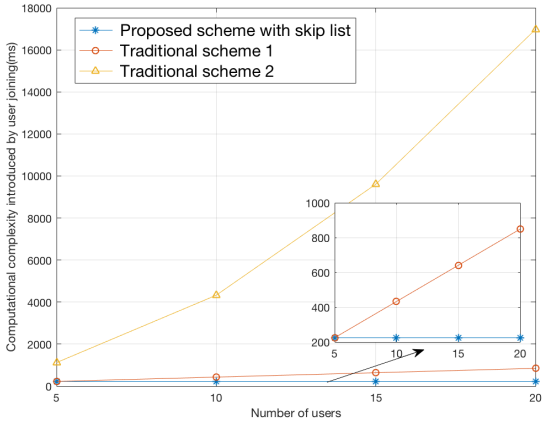


Fig. 3. Computational complexity comparison for user joining

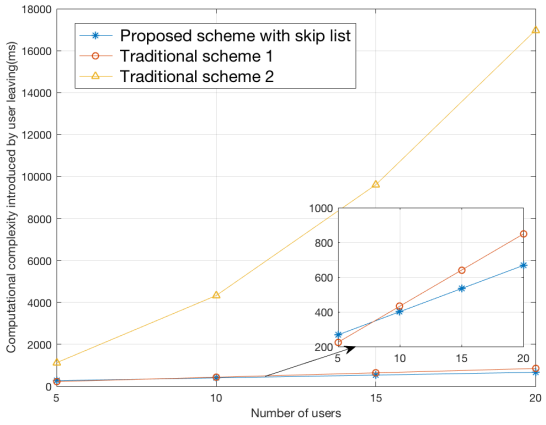


Fig. 4. Computational complexity comparison for user leaving

B. Robustness Against Dishonest Users

In our proposed scheme, as the involved users are divided into $t = \lceil \frac{n}{w} \rceil$ user groups, if there exists one dishonest user in the model aggregation process, only the model updates when one or no more than two user groups are avoided, and the expected scale of the usable model updates is $max(n - (\frac{w*t-n}{n} * 2 * w + \frac{n-(w*t-n)}{n} * w), 0) = max(0, \frac{n^2 - w^2 * t}{n})$. Fig. 5 compares the expected number of model updates to

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TII.2021.3075683, IEEE Transactions on Industrial Informatics

Fig. 5. Comparison of the expected number of updates

the number of users. The comparison results show that our proposed scheme is robust to a dishonest user, while the scheme without a skip list does not detect a dishonest user; i.e., the expected number of remaining models is zero.

C. Trade-off Between Privacy Protection and Computational Complexity

In our proposed scheme, we exploit Eq. (10) to protect each model hyperparameter dimension. For user x_i, if the proposed scheme does not reuse k_i, each piece of the model parameter must be protected by Eq. (2). We exploit the relationship between the scale of key reuse and the key disclosure probability to measure the trade-off between privacy protection and computational complexity. We denote the lower and upper bounds of the value domain D as lb and ub. Using the secret key k_i in one dimension across multiple iterations may lead to the disclosure of both $k_i + ub$ and $k_i + lb$ and further violates the secret key k_i. Thus, from the perspective of one given parameter dimension, we calculate the probability of disclosing key k_i across multiple training iterations.

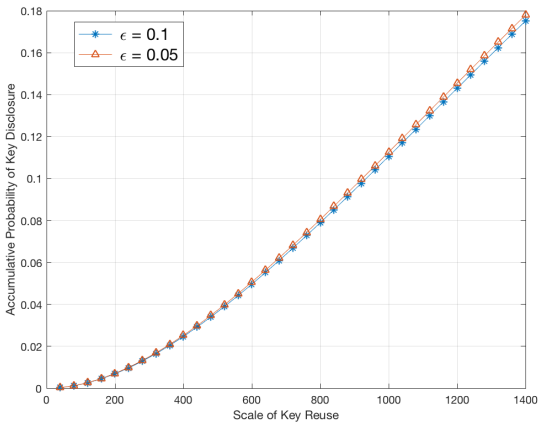


Fig. 6. Exact probability of key disclosure

We let $y_{i,j}^{(t)}$ denote the noise-added parameter $y_{i,j}^{(t)} = m_{i,j}^{(t)} + \sigma_{i,j}^{(t)}$, and the parameter $m_{i,j}^{(t)}$ can be treated as the constant $m_{i,j}$ across some iterations. We use stochastic gradient descent (SGD) to train the NN weights with a relatively small learning rate, and the parameter updates evolve slowly with the iterations [22]. The probability of generating $y_{i,j}^{(t)}$ at iteration t is

$$Pr(y_{i,j}^{(t)}, m_{i,j}) = \frac{\frac{1}{2b} exp(-\frac{|y_{i,j}^{(t)} - m_{i,j}|}{b})}{\sum_{x \in D} \frac{1}{2b} exp(-\frac{|x - m_{i,j}|}{b})}. \quad (11)$$

Given the output $(y_{i,j}^{(1)}, y_{i,j}^{(2)}, ..., y_{i,j}^{(t)})$, the probability of disclosing both the upper bound $k_i + ub$ and the lower bound $k_i + lb$ during the t training iterations is

$$\begin{aligned} &Pr(\textbf{Iteration} = t) = 2 \cdot C_{t-1}^{1} \cdot Pr(lb, m_{i,j}) \\ &\cdot Pr(ub, m_{i,j}) \cdot (1 - Pr(ub, m_{i,j}) - Pr(lb, m_{i,j}))^{t-2}. \end{aligned} \quad (12)$$

Since k_i can also be shared among multiple parameter dimensions during one iteration, the probability of disclosing both $k_i + ub$ and $k_i + lb$ among a group of exactly s parameters is

$$\begin{aligned} Pr(\textbf{Size} = s) = &\sum_{k \in S-s} Pr(lb, m_{i,k}^{(t)}) \cdot Pr(ub, m_{i,s}^{(t)}) \\ &\cdot \prod_{j \in \mathcal{S}-s, j \neq k} (1 - Pr(ub, m_{i,j}^{(t)}) - Pr(lb, m_{i,j}^{(t)})) \\ &+ \sum_{k \in S-s} Pr(ub, m_{i,k}^{(t)}) \cdot Pr(lb, m_{i,s}^{(t)}) \\ &\cdot \prod_{j \in \mathcal{S}-s, j \neq k} (1 - Pr(ub, m_{i,j}^{(t)}) - Pr(lb, m_{i,j}^{(t)})). \end{aligned} \quad (13)$$

Fig. 6 shows the probability of key disclosure concerning the increase in the scale of key reuse. We experiment with the data collected from the smartphone sensor-based vehicular navigation system in [4] and derive the value of the model parameter for testing. Specifically, we build an NN with a rectified linear unit (ReLU) activation function and SGD algorithm for the model parameters, and we derive the upper and lower bounds of the NN with a 95% confidence interval. In our experiment, the level of differential privacy is set to $\epsilon = 0.1$, and the scale of key reuse ranges between 200 and 1000. The evaluation results in Fig. 6 show that when the key is reused for multiple iterations and the parameter is set to the average of all parameters, then the maximum probability of key disclosure is 0.1106 when the key reuse scale is set to 1000. When the key is reused among multiple dimensions and the values of the parameters are chosen randomly, the maximum probability of key disclosure is 0.1122 using the same key reuse scale.

VI. Related Works

In this section, we first review the relevant privacy-preserving model aggregation mechanisms in federated learning, and then we discuss some federated learning-based applications in the vehicular IoT.

A. Privacy-Preserving Secure Aggregation

In federated learning, users maintain private databases on their own devices, and a shared global model is trained under the coordination of a centralized server with the locally processed ephemeral model updates received from users [23],

[24]. As a model update may leak some knowledge about the training samples, some privacy-preserving mechanisms were designed in federated learning for model protection.

The first type of privacy-preserving mechanism in federated learning is achieved through secure multiparty computation. Bonawitz *et al.* [7] proposed a privacy-preserving model aggregation scheme for federated learning that considers training a deep NN with distributed gradient descent across user-held training data on mobile devices. In this scheme, the participating users perform mutual key establishments among themselves, and then they collaborate to calculate an aggregation result. Bonawitz *et al.* [8] proposed a more flexible privacy-preserving aggregation scheme, which is adaptive to varying federated learning scenarios. By combining a secure aggregation protocol and secret sharing techniques, this scheme further supports an arbitrary subset of user dropouts. However, these schemes cannot guarantee the validity of the aggregation result and require secret information exchanges between two users. To solve this problem, Xu *et al.* [10] recently designed a verifiable secure aggregation for the NN training process, which achieves verification of the derived aggregation result. However, the above schemes either do not support user dropout or require all participants to become involved in the key re-establishment process after user dropout.

The second type of hybrid privacy-preserving federated learning mechanism combines differential privacy with secure multiparty computation. Even though the schemes based on secure multiparty computation guarantee the security of the intermediate results, they cannot guarantee the security of the final results, which may also leak an individual part of the model update in the case of collusion. Chase *et al.* [9] combined differential privacy, secure multiparty computation, and secret sharing, which achieves the privacy-preserving training of NNs in a collaborative way. Since the exploitation of differential privacy may lead to poor model performance when there are a large number of users, Truex *et al.* [11] presented a scheme that balances the trade-off between privacy disclosure vulnerability and model performance. In addition, Hao *et al.* [25] brought the homomorphic BGV encryption technique to a noninteractive federated learning scheme, which can resist the collusion of multiple adversarial entities. Liu *et al.* [26] combined homomorphic encryption with secret sharing to propose a federated framework supporting forced aggregation and to be robust against user dropout. Specifically, this scheme resolves the accident user dropout problem without abandoning the current training round. However, these schemes consider only the user dropout situation and do not support the joining of new users, which is highly possible in the vehicular fog scenario with newcomers, and they also waste scarce sensory data from the newcomers.

B. Federated Learning Applications Related to Vehicular Fog

In vehicular fog, users experience high mobility and suffer from intermittent connectivity to each fog server. Lu *et al.* [27] proposed a collaborative federated learning framework on the edges for connected vehicles, which achieves both training time reduction and prediction accuracy. Saputra *et al.* [28] proposed a learning-based solution for energy demand prediction, which realizes energy demand prediction for electric energy networks. However, these schemes mainly focus on formulating models for vehicular applications, and they do not consider the security and privacy preservation of the model updates. Zhao *et al.* [29] proposed another hybrid privacy-preserving mechanism in the IoV, which integrates federated learning with local differential privacy to strengthen the privacy of the model update provided by each vehicle. Lu *et al.* [30] also proposed a privacy-preserving federated learning mechanism to address the data leakage problem in vehicular cyber-physical systems. It also develops a new random subgossip updating scheme to achieve data privacy preservation. However, vehicular systems are experiencing high mobility and intermittent network connections, and it is common for a user to drop out or join the learning process. The above schemes either do not consider the issue of user dropout, or one user dropout may lead to key re-establishment of all participants, which brings heavy computational complexity to the vehicular fog. Meanwhile, these schemes do not consider the joining of newcomers, and they exploit the sensory data to strengthen the learning process.

In contrast, our proposed privacy-preserving model aggregation scheme innovatively exploits a skip list to divide users into groups such that when a user joins or leaves the training process, only the corresponding group members are affected. Although the homomorphic threshold cryptosystem is computationally heavy, we use these complex operations only for key establishments. Meanwhile, the model hyperparameters are further protected by the differential privacy technique. Note that the gist of the proposed privacy-preserving model aggregation scheme is to protect the model updates that are distributively generated by the users, which are equipped with adequate computational power and network connectivity. In this paper, we illustrate the mechanism in the vehicular fog scenario, it can be applied to almost all data-driven fog use cases as long as the basic computation and communication requirements can be satisfied.

VII. Conclusion

In this paper, we proposed a privacy-preserving model aggregation scheme for federated learning-based navigation in vehicular fog. The proposed scheme achieves flexibility and robustness, which supports the dynamic joining and leaving of participants, and is robust against dishonest participants. We performed a security analysis to demonstrate that our proposed scheme satisfies the predefined security requirements for privacy preservation and dishonest user detection. Besides, we carried out extensive experiments and performance evaluations. We showed performance improvements in supporting user joining and leaving and addressing dishonest users. We analyzed the trade-off between privacy protection and computational complexity. In future work, we will consider the implementation of our privacy-preserving model aggregation scheme in a real field test and assess its performance.

ACKNOWLEDGMENT

The work was supported by the National Key R&D Program of China with grant No. 2018YFB1800800, by the Natural Science Foundation of China with grants No. 92067202, No. 62002248, and No. U19A2068, by the China Postdoctoral Science Foundation with grants 2020M671897, No. 2019TQ0217, and No. 2020M673277, by the Key Area R&D Program of Guangdong Province with grant No. 2018B030338001, by Shenzhen Outstanding Talents Training Fund, by Guangdong Research Project No. 2017ZT07X152, by the National Key R&D Program of China with grant No. 2020YFB1805400, by the Provincial Key Research and Development Program of Sichuan with grant No. 20ZDYF3145.

REFERENCES

[1] Q. Kong, R. Lu, F. Yin, and S. Cui, "Privacy-preserving continuous data collection for predictive maintenance in vehicular fog-cloud," *IEEE Trans. Intell. Transp. Syst.*, pp. 1–11, 2020.

[2] J. Wahlström, I. Skog, and P. Handel, "Smartphone-based vehicle telematics: A ten-year anniversary," *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 10, pp. 2802–2825, 2017.

[3] B. V. Philip, T. Alpcan, J. Jin, and M. Palaniswami, "Distributed real-time IoT for autonomous vehicles," *IEEE Trans. Ind. Informatics*, vol. 15, no. 2, pp. 1131–1140, 2019.

[4] F. Yin, Z. Lin, Q. Kong, Y. Xu, D. Li, S. Theodoridis, and S. R. Cui, "Fedloc: Federated learning framework for data-driven cooperative localization and location data processing," *IEEE Open J. of Signal Process.*, vol. 1, pp. 187–215, 2020.

[5] C. Zhu, J. Tao, G. Pastor, Y. Xiao, Y. Ji, Q. Zhou, Y. Li, and A. Ylä-Jääski, "Folo: Latency and quality optimized task allocation in vehicular fog computing," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4150–4161, 2019.

[6] C. Huang, R. Lu, and K. R. Choo, "Vehicular fog computing: Architecture, use case, and security and forensic challenges," *IEEE Commun. Mag.*, vol. 55, no. 11, pp. 105–111, 2017.

[7] K. Bonawitz, V. Ivanov, B. Kreuter, A. Marcedone, H. B. McMahan, S. Patel, D. Ramage, A. Segal, and K. Seth, "Practical secure aggregation for federated learning on user-held data," *CoRR*, 2016.

[8] ——, "Practical secure aggregation for privacy-preserving machine learning," in *Proc. of CCS 2017*, pp. 1175–1191.

[9] M. Chase, R. Gilad-Bachrach, K. Laine, K. E. Lauter, and P. Rindal, "Private collaborative neural network learning," *IACR Cryptol. ePrint Arch.*, p. 762, 2017.

[10] G. Xu, H. Li, S. Liu, K. Yang, and X. Lin, "Verifynet: Secure and verifiable federated learning," *IEEE Trans. Inf. Forensics Secur.*, vol. 15, pp. 911–926, 2020.

[11] S. Truex, N. Baracaldo, A. Anwar, T. Steinke, H. Ludwig, R. Zhang, and Y. Zhou, "A hybrid approach to privacy-preserving federated learning," in *Proc. of AISec@CCS 2019*, pp. 1–11.

[12] N. Holohan, S. Antonatos, S. Braghin, and P. M. Aonghusa, "The bounded Laplace mechanism in differential privacy," *CoRR*, 2018.

[13] G. Karagiannis, O. Altintas, E. Ekici, G. J. Heijenk, B. Jarupan, K. Lin, and T. R. Weil, "Vehicular networking: A survey and tutorial on requirements, architectures, challenges, standards and solutions," *IEEE Commun. Surv. Tutor.*, vol. 13, no. 4, pp. 584–616, 2011.

[14] F. Callegati, W. Cerroni, and M. Ramilli, "Man-in-the-middle attack to the HTTPS protocol," *IEEE Secur. Priv.*, vol. 7, no. 1, pp. 78–81, 2009.

[15] E.-J. Goh, "Encryption schemes from bilinear maps," Ph.D. dissertation, Stanford University, 2007.

[16] W. Pugh, "Skip lists: A probabilistic alternative to balanced trees," in *Algorithms and Data Structures Workshop WADS*, 1989, pp. 437–449.

[17] D. Boneh, X. Boyen, and H. Shacham, "Short group signatures," in *Proc. of Adv. Cryptology 2004*, pp. 41–55.

[18] B. Efron, "Better bootstrap confidence intervals," *J. Am. Stat. Assoc.*, vol. 82, no. 397, pp. 171–185, 1987.

[19] A. M. Zoubir and D. R. Iskander, *Bootstrap techniques for signal processing*, 2004.

[20] A. Ladino, C. Canudas-de-Wit, A. Y. Kibangou, H. Fourati, and M. Rodriguez, "Density and flow reconstruction in urban traffic networks using heterogeneous data sources," in *Proc. of ECC 2018*, pp. 1679–1684.

[21] A. De Caro and V. Iovino, "jpbc: Java pairing based cryptography," in *Proc. of ISCC 2011*, pp. 850–855.

[22] S. Arora, S. S. Du, W. Hu, Z. Li, R. Salakhutdinov, and R. Wang, "On exact computation with an infinitely wide neural net," in *Proc. of NeurIPS 2019*, pp. 8139–8148.

[23] L. Melis, C. Song, E. D. Cristofaro, and V. Shmatikov, "Exploiting unintended feature leakage in collaborative learning," in *Proc. of IEEE SP 2019*, pp. 691–706.

[24] B. Li, Y. Wu, J. Song, R. Lu, T. Li, and L. Zhao, "Deepfed: Federated deep learning for intrusion detection in industrial cyber-physical systems," *IEEE Trans. Industr. Inform.*, 2020.

[25] M. Hao, H. Li, X. Luo, G. Xu, H. Yang, and S. Liu, "Efficient and privacy-enhanced federated learning for industrial artificial intelligence," *IEEE Trans. Ind. Informatics*, vol. 16, no. 10, pp. 6532–6542, 2020.

[26] Y. Liu, Z. Ma, X. Liu, S. Ma, S. Nepal, and R. H. Deng, "Boosting privately: Privacy-preserving federated extreme boosting for mobile crowdsensing," *CoRR*, 2019.

[27] S. Lu, Y. Yao, and W. Shi, "Collaborative learning on the edges: A case study on connected vehicles," in *Proc. of HotEdge 2019*.

[28] Y. M. Saputra, D. T. Hoang, D. N. Nguyen, E. Dutkiewicz, M. D. Mueck, and S. Srikanteswara, "Energy demand prediction with federated learning for electric vehicle networks," in *Proc. of IEEE GLOBECOM 2019*, pp. 1–6.

[29] Y. Zhao, J. Zhao, M. Yang, T. Wang, N. Wang, L. Lyu, D. Niyato, and K. Lam, "Local differential privacy based federated learning for internet of things," *CoRR*, 2020.

[30] Y. Lu, X. Huang, Y. Dai, S. Maharjan, and Y. Zhang, "Federated learning for data privacy preservation in vehicular cyber-physical systems," *IEEE Netw.*, vol. 34, no. 3, pp. 50–56, 2020.

Qinglei Kong (S'15) received received her PhD degree from the School of Electrical and Electronics Engineering, Nanyang Technological University, Singapore, in 2018; the M.Eng. degree in electronic and information engineering from Shenzhen Graduate School, Harbin Institute of Technology, Shenzhen, China, in 2015; and the B.Eng. degree in communication engineering from Harbin Institute of Technology, Harbin, China, in 2012. She used to work in Cyber Security Cluster, Institute for Infocomm Research, Singapore and Tencent Security, Shenzhen, as a research scientist. Now she is working in The Chinese University of Hong Kong, Shenzhen (CUHK-Shenzhen), as a postdoc researcher. Her research interests include applied cryptography, blockchain, VANET, and game theory.

Feng Yin (M'14) received the B.Sc. degree from Shanghai Jiao Tong University, Shanghai, China, in 2008, the M.Sc. and Dr.-Ing. degrees from Technische Universitat Darmstadt, Darmstadt, Germany, in 2011 and 2014, respectively. In 2013, he received the Chinese Government Award for outstanding selffinanced students abroad. In 2014, he received MarieCurie Scholarship from European Union. From 2014 to 2016, he worked at Ericsson Research, Linkoping, Sweden, mainly working on the European Union FP7 Marie Curie Training Programme on Tracking in Complex Sensor Systems. He is currently working at the Chinese University of Hong Kong (Shenzhen) and Shenzhen Research Institute of Big Data in June 2016. His research interests include statistical signal processing, machine learning, and sensory data fusion with applications to wireless positioning and tracking.

Rongxing Lu (S'09-M'11-SM'15-F'20) is an associate professor at the Faculty of Computer Science (FCS), University of New Brunswick (UNB), Canada. Before that, he worked as an assistant professor at the School of Electrical and Electronic Engineering, Nanyang Technological University (NTU), Singapore from April 2013 to August 2016. Rongxing Lu worked as a Postdoctoral Fellow at the University of Waterloo from May 2012 to April 2013. He was awarded the most prestigious "Governor General's Gold Medal", when he received his PhD degree from the Department of Electrical & Computer Engineering, University of Waterloo, Canada, in 2012; and won the 8th IEEE Communications Society (ComSoc) Asia Pacific (AP) Outstanding Young Researcher Award, in 2013. He is presently a senior member of IEEE Communications Society. Dr. Lu currently serves as the Vice-Chair (Conferences) of IEEE ComSoc CIS-TC. Dr.Lu is the Winner of 2016-17 Excellence in Teaching Award, FCS, UNB.

Beibei Li (S'15-M'19) received the Ph.D. degree from the School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore, in 2019. He is currently an Associate Professor with the School of Cyber Science and Engineering, Sichuan University, Chengdu, China. He was invited as a Visiting Researcher with the Faculty of Computer Science, University of New Brunswick, Fredericton, Canada, from March to August 2018. His has authored or coauthored works in IEEE Transactions on Information Forensics and Security, IEEE Transactions on Industrial Informatics, ACM Transactions on Cyber-Physical Systems, IEEE Internet of Things Journal, Automatica, Information Sciences, IEEE ICC, and IEEE GLOBECOM, etc. His current research interests include several areas in security and privacy issues on cyber-physical systems (e.g., smart grids, industrial control systems, etc.), with a focus on intrusion detection techniques, artificial intelligence, and applied cryptography.

Xiaohong Wang is currently a research scientist at the Visual Intelligence cluster, Institute for Infocomm Research in the Agency for Science, Technology and Research (A∗STAR), Singapore. She received the Ph.D. degree (awarded Full Research Scholarship) from the School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore, in 2020; the M.E. degree and B.E. degree from the Central South University, P.R. China in 2014 and 2011, majoring in Biomedical Engineering, respectively. Her research interests mainly focuses on image processing, machine vision and pattern recognition.

Shuguang Cui (S'99-M'05-SM'12-F'14) received his Ph.D. in electrical engineering from Stanford University, California, in 2005. Afterward, he worked as assistant, associate, full, and Chair Professor in Electrical and Computer Engineering at the University of Arizona, Texas A&M University, University of California Davis, and City University of Hong Kong at Shenzhen, respectively. He has also been the Vice Director at Shenzhen Research Institute of Big Data. His current research interests focus on data driven large-scale system control and resource management, large dataset analysis, IoT system design, energy-harvesting-based communication system design, and cognitive network optimization. He was selected as the Thomson Reuters Highly Cited Researcher and listed in the Worlds Most Influential Scientific Minds by ScienceWatch in 2014. He was the recipient of the IEEE Signal Processing Society 2012 Best Paper Award. He has served as General Co-Chair and TPC Co-Chair for many IEEE conferences. He has also served as an Area Editor for IEEE Signal Processing Magazine, and Associate Editor for IEEE Transactions on Big Data, IEEE Transactions on Signal Processing, the IEEE JSAC Series on Green Communications and Networking, and IEEE Transactions on Wireless Communications. He was an elected member of the IEEE Signal Processing Society SPCOM Technical Committee (20092014) and the elected Chair of the IEEE ComSoc Wireless Technical Committee (20172018). He is a member of the Steering Committee for IEEE Transactions on Big Data and the Chair of the Steering Committee for IEEE Transactions on Cognitive Communications and Networking. He was also a member of the IEEE ComSoc Emerging Technology Committee. He was elected as an IEEE Fellow in 2013, an IEEE ComSoc Distinguished Lecturer in 2014, and IEEE VT Society Distinguished Lecturer in 2019.

Ping Zhang (M'05-SM'15-F'19) received the Ph.D. degree from the Beijing University of Posts and Telecommunications (BUPT), Beijing, China, in 1990. He is currently a Professor with the Beijing University of Posts and Telecommunications. He has authored or authored eight books and more than 400 papers, and holds approximately 170 patents. His current research interests include mobile communications, ubiquitous networking, and service provisioning, especially in the key techniques of the 5G systems. He is an Executive Associate Editor-inChief on information sciences of Chinese Science Bulletin, a Member of nextgeneration broadband wireless communication networks in National Science and Technology Major Project Committee, a Member of the fifth Advisory Committee of National Natural Science Foundation of China, the Chief Scientist of "973" National Basic Research Program of China, member of the Ministry of Science and Technology (MOST) 863 Program.