AI-Empowered Trajectory Anomaly Detection for Intelligent Transportation Systems: A Hierarchical Federated Learning Approach

Xiaoding Wang, Wenxin Liu, Hui Lin, Jia Hu, Kuljeet Kaur, *Member, IEEE*, and M. Shamim Hossain, *Senior Member, IEEE*

***Abstract*— The vigorous development of positioning technology and ubiquitous computing has spawned trajectory big data. By analyzing and processing the trajectory big data in the form of data streams in a timely and effective manner, anomalies hidden in the trajectory data can be found, thus serving urban planning, traffic management, safety control and other applications. Limited by the inherent uncertainty, infinity, time-varying evolution, sparsity and skewed distribution of trajectory big data, traditional anomaly detection techniques cannot be directly applied to anomaly detection in trajectory big data. To solve this problem, we propose a hierarchical trajectory anomaly detection scheme for Intelligent Transportation Systems (ITS) using both machine learning and blockchain technologies. To be specific, a hierarchical federated learning strategy is proposed to improve the generalization ability of the global trajectory anomaly detection model by secondary fusion of the multi-area trajectory anomaly detection model. Then, by integrating blockchain and federated learning, the iterative exchange and fusion of the global trajectory anomaly detection model can be realized by means of on-chain and off-chain coordinated data access. Experiments show that the proposed scheme can improve the generalization ability of the trajectory anomaly detection model in different areas, while ensuring its reliability.**

***Index Terms*— Anomaly detection, intelligent transportation systems, federated learning, blockchain.**

I. Introduction

With the development and maturity of sensor network technology, communication technology and positioning technology, various positioning devices and mobile intelligent terminals such as mobile phones have been widely used, realizing large-scale collection of position-related information of moving objects (people, vehicles, ships, etc.). This type of location data contains information such as geographic coordinates, speed, direction, time stamp, etc., and is continuously increased and rapidly updated in the form of time-varying evolution, so it is called trajectory big data [1]. In view of the fact that trajectory big data can be recorded accurately for a long time, and the activities of moving objects within the time range can objectively reflect the activity rules of individual (or groups) of moving objects, it has attracted widespread attention from scholars in many fields such as data science, sociology, and geography. Related research work includes helping people better understand the motion behavior of dynamically evolving objects, predicting their future motion trends, and providing effective support services for location-based social networks, intelligent transportation systems (ITS), urban planning, military reconnaissance and other applications. The application requirements of services are constantly expanding, and the demand for online analysis is increasing, which requires fast processing and response in a relatively short period of time, which means that real-time has become an important feature of trajectory big data [2].

Trajectory data-based pattern discovery aims to extract common features of many moving objects from massive trajectory collections, which helps to discover abnormal patterns in trajectory big data, which is critical in many location-based service applications in ITS. Anomalies, also known as outliers [3], are usually caused by human error, instrument error, heterogeneous data, changes in system behavior. Anomalies are not noise, and while noise is very similar to anomalies, noise can degrade the quality of a dataset. Therefore, in practical applications, denoising is often required in the data preprocessing stage.

Anomaly detection is widely used in databases, data mining, machine learning [4], and statistics, including intrusion detection and fault diagnosis in networks, healthcare monitoring, and public safety emergencies. Taking anomaly detection in urban traffic management as an example, in a saturated urban road network, traffic accidents, bad weather, and road emergencies can lead to congestion or paralysis of the entire road network. Traditional intelligent traffic monitoring detects abnormal traffic flow parameters by deploying magnetic detectors such as video detectors or induction coils. Because such equipment requires expensive infrastructure investment and maintenance expenses, it cannot be densely installed and cover the entire road network, resulting in loss or unreliability of monitoring information in some areas. The real-time anomaly

Manuscript received 1 February 2022; revised 29 June 2022 and 25 August 2022; accepted 16 September 2022. Date of publication 25 October 2022; date of current version 29 March 2023. This work was supported by the King Saud University, Riyadh, Saudi Arabia, through the Researchers Supporting Project number RSP2023R32. The Associate Editor for this article was J. C.-W. Lin. *(Corresponding authors: Hui Lin; M. Shamim Hossain.)*

Xiaoding Wang, Wenxin Liu, and Hui Lin are with the College of Computer and Cyber Security, Fujian Normal University, Fuzhou, Fujian 350117, China, and also with the Engineering Research Center of Cyber Security and Education Informatization, Fujian Province University, Fuzhou, Fujian 350117, China (e-mail: wangdin1982@fjnu.edu.cn; sixwenxin@163.com; linhui@fjnu.edu.cn).

Jia Hu is with the Department of Computer Science, University of Exeter, EX4 4RN Exeter, U.K. (e-mail: j.hu@exeter.ac.uk).

Kuljeet Kaur is with the Electrical Engineering Department, École de Technologie Supérieure, Montreal, QC H3C 1K3, Canada (e-mail: kuljeet.kaur@ieee.org).

M. Shamim Hossain is with the Department of Software Engineering, College of Computer and Information Sciences, King Saud University, Riyadh 11543, Saudi Arabia (e-mail: mshossain@ksu.edu.sa).

Digital Object Identifier 10.1109/TITS.2022.3209903

detection method based on the trajectory data of vehicles in the urban road network can not only discover the abnormality of traffic participants in the path pattern, identify traffic congestion, detect changes in the road network, but also help to update the traffic map.

At present, in-depth research on anomaly detection of trajectory data has found that trajectory big data has the following characteristics, namely uncertainty, sparsity, skewed distribution, large scale, and fast update [5], [6], [7], [8].

- *Uncertainty of trajectory data*: Due to the limited accuracy of positioning technology, as well as the calculation error, signal attenuation and loss of GPS positioning equipment, there are spatial uncertainties in the collected position data. At the same time, different collection frequencies or different time series lengths also bring about time series uncertainty of location data. The uncertainty of space and time series makes the collected trajectory data have a large positional deviation, thus reducing the accuracy of trajectory abnormality detection results.
- *Sparsity and skewed distribution of trajectory data*: Trajectory data reflects the activity law of moving objects, and the activities of moving objects are generally periodic, so the trajectory data often presents uneven distribution. For example, in an urban road network, only a few vehicles pass through certain road sections for a long time, while a few main roads have a large number of vehicles passing through in a short time, which leads to a skewed distribution of trajectory data.
- *Large-scale and rapid update of trajectory data*: Positional data for moving objects is generated in real-time and continues to increase. As long as the moving object is active, the position information will be continuously generated and accumulated, making the amount of trajectory data infinite. Therefore, it is difficult to accurately define the abnormal characteristics of motion behaviors and propose an effective real-time anomaly detection method.

Given the uncertainty, sparsity, skewed distribution, large scale and fast update of trajectory big data, we propose an intelligent trajectory anomaly detection architecture, as shown in Figure 1. The architecture collects vehicle trajectory data through roadside units (RSUs) and aggregates these data into an anomaly detection center for training a local trajectory anomaly detection model. Then, each anomaly detection center uses the local model to train the area trajectory anomaly detection model. Finally, the global anomaly detection center uses the area model to train the global trajectory anomaly detection model.

This paper focuses on solving the following problems of trajectory anomaly detection algorithms, namely the privacy of the data provider cannot be protected during the anomaly detection and the generalization ability of the trajectory anomaly detection model is poor. To this end, under the above architecture, we propose a hierarchical trajectory anomaly detection mechanism using machine learning and blockchain technology for ITS. The main contributions of this paper are as follows:

1) To address the problem of weak generalization ability of the single-area trajectory anomaly detection model, we propose a hierarchical federated learning strategy to improve the generalization ability of the global trajectory anomaly detection model through the secondary fusion of the multi-area trajectory anomaly detection model.
2) To address the problem of untrustworthy training generation of trajectory anomaly detection models, by introducing blockchain technology into federated learning, the iterative exchange and fusion of the global trajectory anomaly detection model can be realized by means of on-chain and off-chain coordinated data access, and the trajectory anomaly detection model can be supervised and aggregated in the federated training process.
3) Experiments show that the proposed scheme can improve the generalization ability of the trajectory anomaly detection model in different areas, while ensuring its reliability.

The rest of this paper is organized as follows. Section II presents the related work. Section III introduces the system model and security model. Section IV gives the implementation details of the proposed scheme. Section V presents the performance evaluation. Section VI concludes this paper.

II. Related Work

Trajectory anomaly detection plays a very important role in intelligent transportation systems. Scholars have carried out research on trajectory anomaly detection from various aspects, and have proposed a large number of excellent solutions.

Qian *et al.* [9] first defined two spatiotemporal models to characterize the relationship between displacement and travel distance/travel time, and identified the point as an anomaly if travel time and travel distance were not within the normal range. Then, the similarity of traffic patterns in different time periods and neighboring areas was used to improve detection efficiency and reduce the number of models that need to be learned. Ahmed *et al.* [10] utilized the network structure and the neighbors of nodes to build structural embeddings through inter-node relationships, and then implemented a method to learn latent representations of biased points in the road network structure by employing random walks in a hierarchical multi-layer graph to generate a set of Sequence to adjust the node embedding to obtain the journey embedding, and finally used LSTM to cluster the embedding to discover the trajectory deviation points. Xu *et al.* [11] represented network traffic data as tensors and obtained spatial and multi-scale temporal patterns of traffic changes through sliding window tensor decomposition, then identified different anomaly types by measuring deviations from different spatial and temporal patterns, and finally solved for anomalies chained best matching paths to discover path-level anomalies. To address the taxi fraud problem, Belhadi *et al.* [12] proposed a strategy for identifying trajectory outliers for identifying individual and group outliers. For single trajectory outliers, it was judged by calculating the distance of each point in each trajectory, while for group trajectory outliers it was achieved by using feature selection and sliding window strategies. Then, they proposed an algorithm based on hybrid data mining [13], which first applied a clustering algorithm to construct micro-clusters, then combined the k-NN algorithm to calculate outlier candidates, and finally used a pattern mining framework as a pruning strategy to generate outlier groups. Santhosh *et al.* [14] proposed trajectory classification and anomaly detection using a hybrid convolutional neural network and variational autoencoder architecture, where color gradient representations introduced

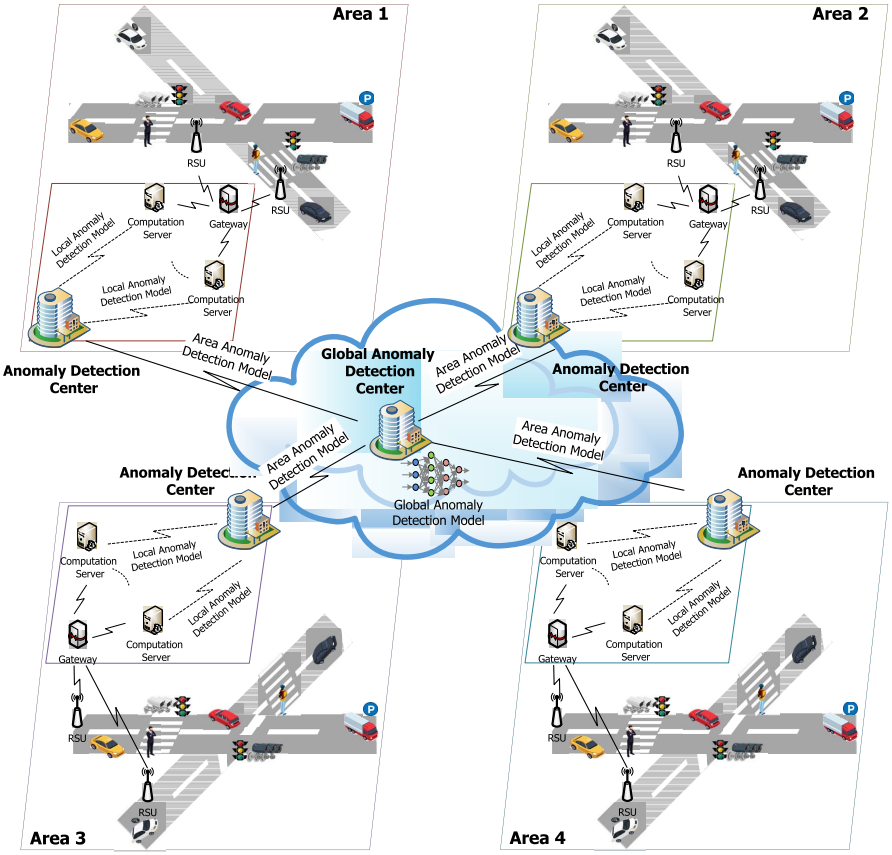

Fig. 1. A novel hierarchial trajectory anomaly detection architecture for ITS.

high-level features for object trajectories of different lengths, and a time-incremental gravity model was used to extract moving objects trajectory. Rovatsos *et al.* [15] adopted a quickest change detection framework, assuming it is assumed that the anomaly evolution is unknown but deterministic. They modified the Loden detection delay to obtain anomaly trajectories that maximize the delay of the detection process, and the cumulative sum test and its improved version can be used to solve the problem of time series data anomalies under homogeneous and heterogeneous sensors. Wang *et al.* [16] used disparity and intersection set distance metrics to evaluate the similarity between trajectories, quantifying the differences between different types of anomaly trajectories and normal trajectories on this basis, and propose an trajectory anomaly detection method to find different anomalies. To detect anomalies, Cho *et al.* [17] used multi-output Gaussian process regression to probabilistically predict the output of the target system, and then detected system anomalies by comparing the predicted responses with the measurements of the target system, where the Mahalanobis distance between trajectories exceeds the extreme value theoretical threshold then the trajectory is anomaly. Ding *et al.* [18] proposed a heuristic maximum fraud trajectory construction algorithm and a fraud detection algorithm to detect anomaly taxi trips. The algorithm detects fraudulent trips on synthetic, real trajectory datasets, without the assistance of a meter. Qiao *et al.* [19] analyzed pedestrian trajectories from the perspectives of clustering, bias and trajectory entropy, thereby proposing an anomalous trajectory identification framework, in which the improved K-Means method was used for the clustering of pedestrian destinations and trajectories, while the Mahalanobis distance It is used to evaluate the trajectory deviation, and the dimensional characteristics are established by the speed and angle difference of the trajectory. Li *et al.* [20] proposed a classifier based on a spatio-temporal cascaded autoencoder to explore the spatial and temporal correlations of video data, where the spatiotemporal adversarial autoencoder obtains a Gaussian model to fit regular data, while a spatiotemporal convolutional autoencoder classifies each specific anomaly via reconstruction error, a two-stream framework fuses appearance and motion cues for more reliable detection results. Mothukuri *et al.* [21] proposed an implementation of the detection of attacks in the IoT through federally trained GRU models and guarantee the accuracy of the global attack detection model by aggregating the detection model updates from multiple data sources. Połap *et al.* [22] proposed an alternative structure for federated learning in which private data of participants can be sent to the server with the best classification results for optimization in the samples of other participants if they satisfy certain conditions. The server collects these data as having the best classification results and returns them and receives new enhanced data in return through GAN. Ahmed *et al.* [23] proposed a graph-based algorithm for anomalous trajectory detection and classify the trajectories using machine learning algorithms on the features of the graph. Belhadi *et al.* [24] proposed two types of anomalous behavior detection algorithms. First, algorithms based on data mining and knowledge discovery that study different correlations between human behavioral data and identify collective human anomaly behaviors from the extracted knowledge. Second, algorithms that explore convolutional deep neural networks to identify collective anomaly human behavior by learning different features of historical data.

Although the above research work has made great contributions to the detection of anomaly trajectories in intelligent transportation, it still needs to face the following two challenges: (i) How to ensure the privacy of data providers in the process of trajectory anomaly detection? (ii) How to effectively improve the generalization of anomaly detection model so that it can be applied to different areas and different anomaly detection tasks? To address these two challenges, this paper proposes a hierarchical deep federated learning strategy for privacy-preserving, highly generalizable trajectory anomaly detection.

III. System Model

A. System Model

The system architecture considered in this scheme is centralized hierarchical federated learning. Centralized federated learning is used because it provides higher efficiency and centralization provides higher robustness compared to a peer-to-peer structure, including the following roles, namely area fusion server S_a, global fusion server S_g, anomaly detection task issuer TI, federated learning participant P_n and IPFS server S_{ipfs}, Trust key issuer I_{key}, as shown in Figure 2.

- *Anomaly detection task issuer* belongs to a certain area and is responsible for issuing trajectory anomaly detection tasks.
- *Participants* are multiple computing servers in a area, which are responsible for collecting trajectory data of traffic participants and training local trajectory anomaly detection models in these trajectory data to detect traffic participants with anomaly trajectories.
- *Area fusion server* is the anomaly detection center in each area and is responsible for aggregating the local trajectory anomaly detection models in its area to generate a area trajectory anomaly detection model.
- *Global fusion server* is the global anomaly detection center and is responsible for aggregating individual area trajectory anomaly detection models to generate a global trajectory anomaly detection model. The global anomaly detection model is a more generalized anomaly detection model compared to the local anomaly detection model and the area anomaly detection model, which can achieve trajectory anomaly detection in multiple areas at the same time.
- *IPFS server* is responsible for persistent storage of the models generated in federated learning by storing the unique content-ID (Content-ID, CID) returned by the models. Since the IPFS system is content-based addressing, the CID is generated by a hash function based on the stored content.
- *Trust key issuer* is responsible for issuing key pairs (pk, pr) to registered entities in the federated learning. The public key pk is published in the blockchain network to verify the signature; the private key pr is kept secretly locally and is used to sign the data.

In this paper, two smart contracts need to be constructed for model fusion, namely the area model fusion smart contract SC_r and the global model fusion smart contract SC_g. The contract SC_r is constructed by the participants in each area and the area fusion server, and executes the upload of the local model, while the contract SC_g is constructed by the area fusion server and the global fusion server and executes the upload of the area model. To save storage resources on the blockchain, we use an on-chain and off-chain collaborative approach to perform federated learning. That is, all models built during federated learning will be stored in the IPFS server, and the fixed-length CIDs obtained by storing the models will be stored on the blockchain. Entities that need model fusion download the corresponding model in IPFS through the model CID on the blockchain for fusion. Furthermore, regarding the generalization ability of the trajectory anomaly detection model, we define it as the ability to correctly detect anomalous trajectories when performing the trajectory detection task after transferring the trajectory anomaly detection model from one area to another.

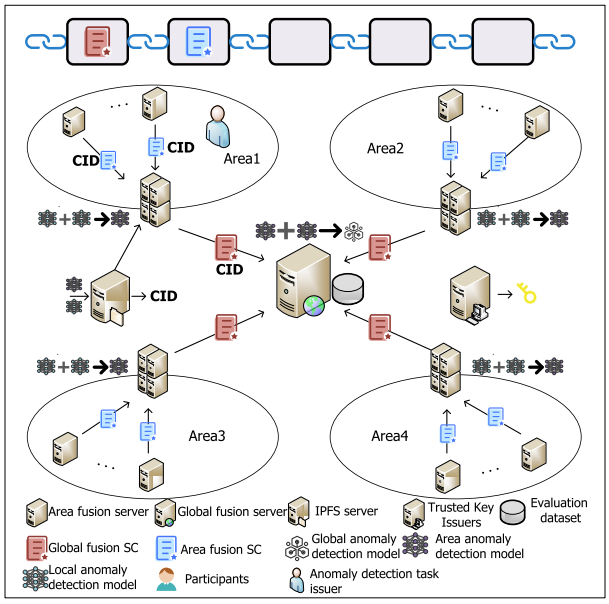

Fig. 2. System model of hierarchical trajectory anomaly detection.

B. Security Model

This paper mainly focuses on the following two threats, namely the threat of privacy leakage and the threat of model unreliability.

- *Privacy Leakage Threat*: Since the trajectory data of traffic participants may contain relevant private data, the curious data computing center will lead to the leakage of private information in the trajectory data during the trajectory anomaly detection process.
- *Model Unreliability Threat*: During the process of building a global trajectory anomaly detection model, there will be lazy participants submitting unreliable models or trajectory data, resulting in an unreliable global anomaly detection model.

Therefore, in the process of performing trajectory anomaly detection, it is necessary to protect the trajectory data to prevent the leakage of relevant private data of traffic participants, and at the same time introduce a monitoring mechanism for traffic participants and a traceability mechanism for model reliability.

The main symbols and their meanings of the proposed scheme are shown in Table I.

TABLE I
MAIN SYMBOLS AND MEANINGS

Symbol	Meaning
TI	Task issuer
P_n^a	Participant
S_a	Area fusion server
S_g	Global fusion server
S_{ipfs}	IPFS server
I_{key}	Trust key issuer
(pk, pr)	key pair
${}^t w_n^a$	Local anomaly detection model
${}^t w^a$	Area anomaly detection model
${}^t W$	Global anomaly detection model
SC_a	Area model fusion smart contract
SC_g	Global model fusion smart contract
λ	Fusion weight

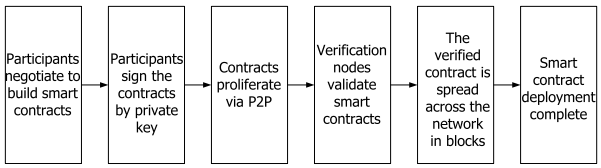

Fig. 3. Smart contract construction and deployment.

IV. IMPLEMENTATION DETAILS OF THE PROPOSED SCHEME

The blockchain-based hierarchical federated learning scheme mainly includes two parts, namely federated learning within trust areas and federated learning among trust areas. Intra-trust area federated learning is a federated learning performed between a area fusion server and participants in different areas to generate a trust area model. The federated learning between trusted areas is to perform federated learning between the global fusion server and multiple area fusion servers to generate a trusted global model.

Specifically, the proposed hierarchical federated learning requires the construction of two trajectory anomaly detection models, namely an area trajectory anomaly detection model and a global trajectory anomaly detection model. The former one is constructed through intra-area federated learning to perform the task of trajectory anomaly detection in a fixed area. However, this model has poor generalization ability. In contrast, the later one is constructed by cross-area federated learning, which has good generalization ability and can be applied to trajectory anomaly detection tasks in each area (including the one that is unable to detect trajectory anomaly).

A. Trusted Intra-Area Federated Learning

Before performing federated learning in a trusted area, the area participants need to build the area model fusion smart contract SC_a with the area fusion server. The contract construction process is shown in Figure 3. First, the participants and the area fusion server build a smart contract SC_a, and the builder needs to sign the contract SC_a, which will be broadcast to all nodes via P2P. Next, the verification nodes (miners) in the blockchain network verify the contract SC_a, and the verified contract SC_a is packaged into a new block and recorded on the longest blockchain. Thus, the deployment of the contract SC_a is complete. The contract SC_a specifies the type of data submitted by the participant, limits the time for local training, and opens an interface for uploading data to the participant. After the contract is deployed, the federated learning in the area is set in motion.

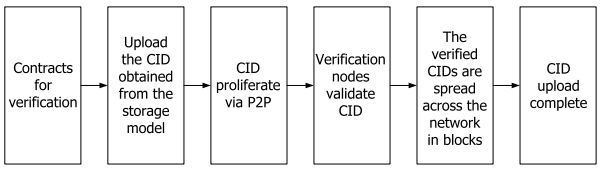

Fig. 4. CID upload process.

Participants train on the local dataset D_n^a to generate a local model ${}^t w_n^a$. The process of participant P_n^a local training can be defined as follows:

$$ {}^t w_n^a = LT({}^t w^a, D_n^a, Adam), \tag{1} $$

where $LT(\cdot)$ represents the local training process used by the participant, $Adam$ is the optimizer used to perform local model training.

When participants complete the local training, the model will be signed, and the signature $Sig_{pr_n^a}({}^t w_n^a)$ will be stored together with the model ${}^t w_n^a$ in the IPFS server. Meanwhile, the IPFS server will return the unique identification of the corresponding storage content. Then, the participant P_n^a call the area model fusion smart contract SC_a, and the contract will verify participants' legitimacy, and check whether the local training time has expired. Next, the local model and the signatures of participant P_n^a will be submitted to the smart contract SC_a, while participants upload the CID of the local model through the upload interface, and broadcast it to all nodes through P2P. Next, the CID is verified by validating nodes (miners) in the blockchain, and it is packaged into a new block and recorded on the longest blockchain. At this point, the local model CID upload is complete as shown in Figure 4.

When the CID upload is complete, the area fusion server S_a calls the contract SC_a, downloads the local model from the IPFS server according to the CID in the blockchain, and verifies the signatures of all participating models again. After verification, the area fusion server S_a fuses all local models to generate the area model ${}^t w^a$ of the current federated learning in the area. The area model fusion algorithm adopts FedAvg, i.e., ${}^t w^a = \frac{1}{N} \sum_n^N {}^t w_n^a$, where N is the number of local models. We then summarize the intra-area federated learning in Algorithm 1.

Algorithm 1 Trusted Intra-Area Federated Learning

Require: Area model fusion smart contract SC_a,
Ensure: Area anomaly detection model ${}^t w^a$
1: **for** participants in area a **do**
2: Participant P_n^a train locally to generate the local model ${}^t w_n^a$.
3: Participant store local model ${}^t w_n^a$ to obtain the CID, and upload the CID to blockchain via SC_a.
4: **end for**
5: The miner performs verification, and generates a new block.
6: The area fusion server S_a downloads the local models from the IPFSs based on the CID stored in the blockchain.
7: The area fusion server S_a merge local models into the area model ${}^t w^a$.

Since the blockchain is traceable and immutable, the verified and on-chain CID will not be tampered with and can be traced forever. When the task issuer needs to audit the process of federated learning, blockchain and IPFS can well help him audit

the model data generated in federated learning. In addition, IPFS is content-addressable, and CIDs are generated based on the hash function of the stored content. Once a participant uploads the CID, the corresponding model cannot be tampered with. Therefore, intra-area federated learning is credible.

B. Trusted Inter-Area Federated Learning

Before performing federated learning between trusted areas, the global fusion server S_g and the area fusion server S_a build a global model fusion smart contract SC_g, which opens the interface for the area fusion server to submit data. When all areas have completed intra-area federated learning, each area fusion server stores the signatures and area models in the IPFS server to obtain the CIDs. Then, each area fusion server uploads the area model CID to the blockchain through SC_g.

Note that the inter-area federated learning is designed to aggregate area models only to generate the global model. When all area fusion servers complete uploading, the global fusion server S_g first calls the contract SC_g, then downloads the corresponding models from the IPFS server and verifies the signatures of them. The verified areas model are fused into the global model ${}^tW$ at the current round t of the federated learning. Only when the prediction accuracy of the model ${}^tW$, denoted by $Acc({}^tW)$, on the evaluation dataset reaches the preset threshold θ, the federated learning ends such that the model ${}^tW$ is the final trajectory anomaly detection model. The inter-area federated learning is summarized in Algorithm 2.

Algorithm 2 Trusted Inter-Area Federated Learning

Require: Global model fusion smart contract SC_g,
Ensure: Global anomaly detection model ${}^tW$

```
while the prediction accuracy Acc(tW) is lower than threshold θ do
    for each area a do
        Area fusion server S_a performs Trusted Intra-Area Federated Learning.
        Area fusion server S_a stores the area model tw^a to obtain the CID, and upload it to the blockchain via SC_g.
    end for
    The miner performs verification, and generates a new block.
    The global fusion server S_g downloads the area models from the IPFS based on the CID stored in the blockchain.
    The global fusion server S_g fuses area models to generate the global model tW at round t.
end while
```

Like intra-area federated learning, blockchain and IPFS are introduced in the inter-area federated learning process to make it trustworthy, traceable, and tamper-proof.

C. Inter-Area Model Weighted Fusion Strategy

Since the task issuer needs to ensure the reliability of the global model for the trajectory anomaly detection service of the area a, it is necessary to reduce the loss of the reliability of the area model during the fusion process, thereby improving the generalization ability of the global model. To this end, we propose a weighted fusion strategy of inter-area models. In the fusion process of area models, the weight of each area model is determined by the degree of deviation between the model and the model in the area where the task issuer is located, that is, the greater the deviation, the lower the weight. For convenience, we call the model in the area where the task issuer is located as the target model, and the models in other areas as other models.

During the area model fusion, we let all the area models to be aggregated in the global fusion server S_g consist of the set Set^t, i.e.,

$$Set^t = \{{}^tw^a | a \in A\}, \tag{2}$$

where A represents the set of area a. Since the Euclidean distance can visually reflect the distance between models in space, while the cosine similarity only considers the direction of the model tensor. Therefore, Euclidean distance is used as a measure of the difference between models. Let the Euclidean distance $Ed^a_{a'}$ between other models ${}^tw^{a'}$ and the target model ${}^tw^a$ be calculated by

$$Ed^a_{a'} = \sqrt{({}^tw^{a'} - {}^tw^a)^2}. \tag{3}$$

On this basis, for models ${}^tw^{a'}$, we calculate the weights $\lambda^{a'}$ in fusion by

$$\lambda^{a'} = \delta \cdot \frac{Ed^a_{a'}}{\sum_{a'}^{R} Ed^a_{a'}}, \tag{4}$$

where δ indicates that the weight coefficient is a value between 0 and 1. Obviously, the weight λ^a for the target model in fusion equals to $\lambda^a = 1 - \delta$. Then, the global fusion server S_g aggregates all area models, and generates a global model ${}^tW$ of inter-area federated learning by

$${}^tW = \delta \cdot \sum_{a}^{A} \lambda^{a'} \cdot {}^tw^{a'} + (1 - \delta) \cdot {}^tw^a. \tag{5}$$

In this paper, we set the number of rounds of inter-domain federated learning to R, that is, the scheme ends after R rounds of inter-area federated learning are executed, thus producing the final federated learning global model ${}^RW$. Furthermore, whether it is intra-area federated learning or inter-area federated learning, all models need to be sent to the relevant servers for fusion. Therefore, we do not strictly require synchronization, but only require that all in-domain participants or area fusion servers participating in the task need to upload the model.

D. Trajectory Anomaly Detection Based on Hierarchical Federated Learning

In this section, we present an anomalous trajectory detection scheme based on hierarchical federated learning, as follows.

- *Step 1:* The task issuer publishes the trajectory anomaly detection task.
- *Step 2:* Each anomaly detection center is established as a computing center within its area.
- *Step 3:* Each computing center trains the local trajectory anomaly detection model according to the collected local trajectory data.

- *Step 4:* Each computing center stores the model and uploads the CID of the local model. Validation nodes (miners) perform relevant validations and record the CIDs of these local anomalous trajectory detection models as new blocks in the blockchain.
- *Step 5:* Each anomaly detection center downloads the local trajectory anomaly detection model according to its CID, and aggregates it to generate the new area trajectory anomaly detection model of each area.
- *Step 6:* Each anomaly detection center completes the storage of the area trajectory anomaly detection model and the upload of the CID. Verification nodes (miners) perform relevant verification and record the CIDs of the trajectory anomaly detection models in these areas as new blocks in the blockchain.
- *Step 7:* The global anomaly detection center downloads the area trajectory anomaly model according to the CID of the area trajectory anomaly detection model and aggregates it to generate the global trajectory anomaly detection model.
- *Step 8:* The global anomaly detection center evaluates the global anomaly detection model. If the model meets the requirements, the federated learning ends; otherwise, a new round of federated learning will be performed.
- *Step 9:* The task issuer performs the trajectory anomaly detection task through the global anomaly detection model.

The federated learning scheme generates the final global trajectory anomaly detection model by secondary fusion of area models with different characteristics in different areas, which improves the generalization ability of the original single-area model. At the same time, we propose a weighted fusion method to reduce the loss of service reliability of the target area after the fusion of different area models, improve the generalization ability of the global trajectory anomaly detection model, and ensure the reliability of the model. Furthermore, since the data exchange between different fusion servers is still generated by the local models trained by the participants, the proposed hierarchical federated learning scheme can still provide the same local data privacy protection as traditional federated learning.

V. Experiment

A. Experiment Setup

In this section, we comprehensively evaluate the proposed scheme through the scientific computing libraries Tensorflow in python. The experimental environment is configured on the computer of Intel(R) Core(TM) i5-10300H CPU @ 2.50GHz and RTX2060 6G, and the version of Tensorflow used is 2.2.0. In addition, we deployed a 4-node blockchain network through FISCO BSCO in the virtual machine of ubuntu20.04 for the verification of the proposed blockchain scheme.

The anomaly detection model in the simulation experiments is a two-layer neural network model, as shown in Table II. The first layer is the LSTM layer, containing 64 neural units with tanh activation and sigmod recurrent activation; the second layer is the Dense layer, containing 7 neural units.

In this paper, the real-world traffic flow dataset NGSIM, which is available at "`https://ops.fhwa.dot.gov/trafficanalysistools/ngsim.htm`", is used to learn a trajectory anomaly detection model. The NGSIM dataset has been widely used in the field of traffic flow simulation. It consists of vehicle dynamic information collected by cameras arranged along the road in different time periods, including vehicle speed, acceleration, and position coordinates. In addition, this paper uses the data-driven texture synthesis method proposed in [25] to synthesize six types of traffic trajectories including normal driving, sudden acceleration, long-term stop, frequent shifting, left-right swing and reverse driving by controlling parameter settings as test sets, and the proportion of abnormal trajectories is about 5%.

TABLE II
Anomaly Detection Model

Layer	Type	Units	Activation
First Layer	LSTM	64	tanh/sigmod
Second Layer	Dense	7	-

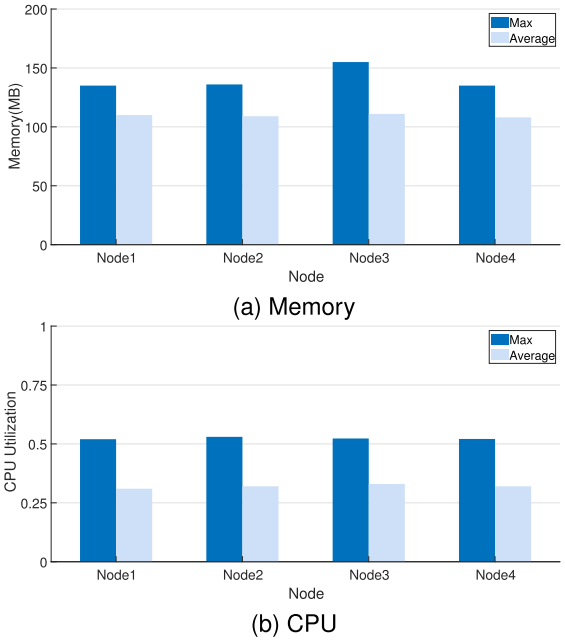

Fig. 5. Data download.

The experiment simulates federated learning between two areas, area A and area B, with 2 participants in each area. The task issuer is in area A, and entrusts the global model fusion server to aggregate different models in the two fields to generate the final global model.

B. Experiment Result

Figure 5(a) and (b) show the cpu utilization and memory consumption of each node when testing the download interface after deploying the area model fusion smart contract SC_a and the global model fusion smart contract SC_g in a 4-node blockchain network. As shown in figure 5(a), the maximum memory usage of node 0 to node 3 is 76.7mb, 77.3mb, 74.6mb and 75.2mb, respectively; the average memory usage is 76.6mb, 77.3mb, 74.5mb and 75.2mb, respectively. As shown in Figure 5(b), the maximum CPU usage of node 0 to node 3 is 15.2%, 13.8%, 15.6% and 14.6%; the CPU occupancy was 12.2%, 11.4%, 12.2% and 11.2%.

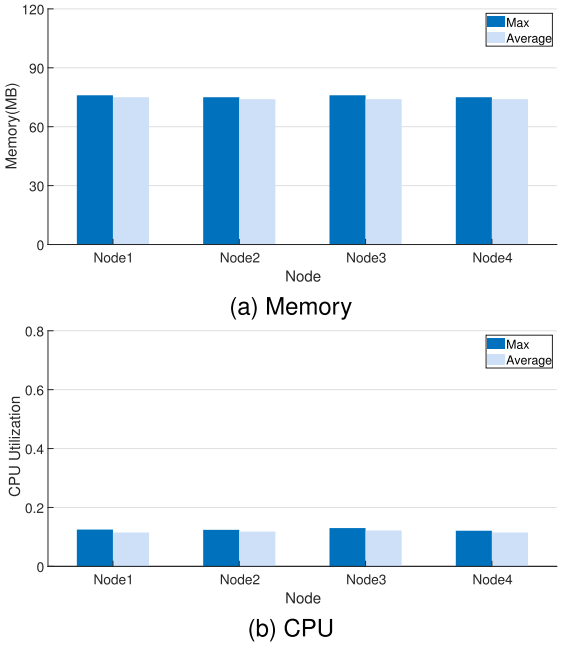

Fig. 6. Data upload.

Figure 6 (a) and (b) show the cpu utilisation and memory consumption of each node when testing the upload interface after deploying the area model fusion smart contract SC_a and the global model fusion smart contract SC_g in a 4-node blockchain network. As shown in Figure 6(a), the highest memory usage of node 0-node 3 is 135.4mb, 135.3mb, 154.0mb and 135.6mb, respectively; the average memory usage is respectively 108.9mb, 109.6mb, 111.9mb and 107.3mb. As shown in Figure 6(b), the highest CPU occupancy rates of node 0-node 3 are 54%, 60%, 58% and 58.2%, respectively; the CPU occupancy rates are 36%, 39.3%, 39.7% and 40.9%, respectively. In summary, it can be seen that the upload interface consumes more resource node resources compared to the download interface.

The intra-area federated learning and the inter-area federated learning in area A under the proposed scheme are evaluated, and the results are shown in Figure 7, where the evaluation dataset is the area A's evaluation data. It is clearly that with the increase of the number of federated learning rounds, the area A model continuously learns the local data features of each participant in the area, and the area A model has an increasing anomaly detection accuracy in the evaluation dataset. For the global model, since other area models will be aggregated, the anomaly detection accuracy on the evaluation dataset of area A is at a low level of only about 20% at the beginning. With the inter-area federated learning round increases, the anomaly detection accuracy of the global model on area A's evaluation dataset increase, and finally is almost as high as that of the original model in area A. However, since the other area models are aggregated to construct the global model, the detection accuracy will be slightly lower than that of the original area model by about 2%, which is acceptable.

As shown in the Table III, trajectory anomaly detection comparison between the proposed scheme and the baselines CNN-GPSTasST [26] and CNN-VAE [14] in terms of Accuracy, Recall and F1 during the federated learning. Observed from the comparison results, we find that with the increase of the number of federated learning rounds, the anomaly

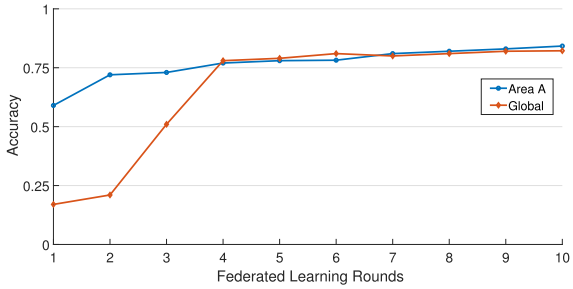

Fig. 7. Federated learning performance.

TABLE III
ANOMALY DETECTION MODEL COMPARISON

Schemes	Indexes	3 rounds	5 rounds	10 rounds
CNN-GPSTasST [26]	Accuracy	79.3%	82.6%	84.2%
	Recall	45.3%	70.3%	75.4%
	F1	41.2%	73.5%	78.6%
CNN-VAE [14]	Accuracy	80.4%	83.7%	84.5%
	Recall	45.2%	71.2%	76.7%
	F1	43.4%	74.3%	82.5%
This paper	Accuracy	76.3%	71.7%	85.7%
	Recall	61.6%	83.7%	83.8%
	F1	69.4%	76.9%	84.8%

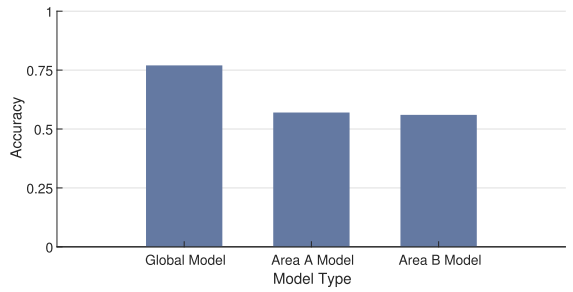

Fig. 8. Model generalization.

detection model in this scheme can reach 85.7%, 83.8%, and 84.8% respectively in each index, which are higher than 84.2%, 75.4%, and 78.6% of CNN-GPSTasST and 84.5%, 76.7%, and 82.5% of CNN-VAE after 10 rounds' federated learning. As we expected, all baselines perform worse than the proposed scheme simply because the proposed scheme is designed to build a trajectory anomaly detection model with strong generative ability by introducing a weighted fusion method, while comparing with the baselines.

The model's generalization ability is evaluated in Figure 8, and the evaluated dataset is the fusion dataset of each area evaluation dataset. As shown in Figure 8, since the training data of the area models of area A and area B are limited to the areas where they are located, the features learned by the area models are relatively less, so the prediction accuracy in large-scale evaluation dataset is lower, thereby the generalization ability of the model is not high. The global model constructed by this scheme improves the generalization ability of the model through the secondary weighted aggregation of different area models. Therefore, in the process of large-scale data evaluation, the global model constructed by this scheme has higher prediction accuracy than the area A model and the area B model, which suggests it has a higher generalization ability.

The experimental results show that the scheme proposed in this paper improves the generalization ability of the model while ensuring the reliability of the global model, meanwhile it can ensure the credibility of the federated learning.

VI. Conclusion

The rapid popularization of mobile Internet and smart devices equipped with positioning systems has led to the rapid accumulation of trajectory data. Therefore, mining useful information from large-scale trajectory data has become a hot spot in the field of smart transportation research in recent years. Detecting abnormal trajectories of vehicles in cities is often limited by the inherent uncertainty, infinity, time-varying evolution, sparsity and skewed distribution of trajectory big data, which makes traditional anomaly detection techniques unable to be directly applied to anomaly detection for trajectory big data. To solve this problem, this paper proposes a hierarchical trajectory anomaly detection scheme for intelligent transportation systems using machine learning and blockchain technology. Specifically, a hierarchical federated learning strategy is proposed to improve the generalization ability of the global trajectory anomaly detection model by secondary fusion of the multi-area trajectory anomaly detection model. Then, through the fusion of blockchain and federated learning, the iterative exchange and fusion of the global trajectory anomaly detection model is achieved through on-chain and off-chain collaborative data access. Experiments show that this scheme can improve the generalization ability of the trajectory anomaly detection model in different areas, while ensuring its reliability.

Due to the new threat of privacy leakage in federated learning, future research directions will consider designing trajectory anomaly detection methods with fine-grained privacy-preserving mechanisms. At the same time, the problem of optimizing asynchronous federated learning from the perspective of privacy protection will be considered.

References

[1] B. Qu, W. Yang, G. Cui, and X. Wang, "Profitable taxi travel route recommendation based on big taxi trajectory data," *IEEE Trans. Intell. Transp. Syst.*, vol. 21, no. 2, pp. 653–668, Feb. 2020.

[2] S. Li, L. Yang, and Z. Gao, "Efficient real-time control design for automatic train regulation of metro loop lines," *IEEE Trans. Intell. Transp. Syst.*, vol. 20, no. 2, pp. 485–496, Feb. 2019.

[3] A. R. Javed, M. Usman, S. U. Rehman, M. U. Khan, and M. S. Haghighi, "Anomaly detection in automated vehicles using multistage attention-based convolutional neural network," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 7, pp. 4291–4300, Jul. 2021.

[4] X. Hu, Y. Zhang, X. Liao, Z. Liu, W. Wang, and F. M. Ghannouchi, "Dynamic beam hopping method based on multi-objective deep reinforcement learning for next generation satellite broadband systems," *IEEE Trans. Broadcast.*, vol. 66, no. 3, pp. 630–646, Sep. 2020.

[5] M. Shao, J. Li, Q. Yan, F. Chen, H. Huang, and X. Chen, "Structured sparsity model based trajectory tracking using private location data release," *IEEE Trans. Depend. Sec. Comput.*, vol. 18, no. 6, pp. 2983–2995, Dec. 2021.

[6] J. J. Xu *et al.*, "Trajectory big data: Data, applications and techniques," *J. Commun.*, vol. 36, no. 12, p. 97, 2015.

[7] D. Xia *et al.*, "Discovering spatiotemporal characteristics of passenger travel with mobile trajectory big data," *Phys. A, Stat. Mech. Appl.*, vol. 578, Sep. 2021, Art. no. 126056.

[8] D. R. de Almeida, C. de Souza Baptista, F. G. de Andrade, and A. Soares, "A survey on big data for trajectory analytics," *ISPRS Int. J. Geo-Inf.*, vol. 9, no. 2, p. 88, 2020.

[9] S. Qian *et al.*, "Detecting taxi trajectory anomaly based on spatio-temporal relations," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 7, pp. 6883–6894, Jul. 2022, doi: 10.1109/TITS.2021.3063199.

[10] U. Ahmed, G. Srivastava, Y. Djenouri, and J. C.-W. Lin, "Deviation point curriculum learning for trajectory outlier detection in cooperative intelligent transport systems," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 9, pp. 16514–16523, Sep. 2022, doi: 10.1109/TITS.2021.3131793.

[11] M. Xu, J. Wu, H. Wang, and M. Cao, "Anomaly detection in road networks using sliding-window tensor factorization," *IEEE Trans. Intell. Transp. Syst.*, vol. 20, no. 12, pp. 4704–4713, Dec. 2019.

[12] A. Belhadi, Y. Djenouri, G. Srivastava, D. Djenouri, A. Cano, and J. C.-W. Lin, "A two-phase anomaly detection model for secure intelligent transportation ride-hailing trajectories," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 7, pp. 4496–4506, Jul. 2021.

[13] A. Belhadi, Y. Djenouri, G. Srivastava, A. Cano, and J. C.-W. Lin, "Hybrid group anomaly detection for sequence data: Application to trajectory data analytics," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 7, pp. 9346–9357, Jul. 2022, doi: 10.1109/TITS.2021.3114064.

[14] K. K. Santhosh, D. P. Dogra, P. P. Roy, and A. Mitra, "Vehicular trajectory classification and traffic anomaly detection in videos using a hybrid CNN-VAE architecture," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 8, pp. 11891–11902, Aug. 2022, doi: 10.1109/TITS.2021.3108504.

[15] G. Rovatsos, G. V. Moustakides, and V. V. Veeravalli, "Quickest detection of moving anomalies in sensor networks," *IEEE J. Sel. Areas Inf. Theory*, vol. 2, no. 2, pp. 762–773, Jun. 2021.

[16] J. Wang *et al.*, "Anomalous trajectory detection and classification based on difference and intersection set distance," *IEEE Trans. Veh. Technol.*, vol. 69, no. 3, pp. 2487–2500, Mar. 2020.

[17] W. Cho, Y. Kim, and J. Park, "Hierarchical anomaly detection using a multioutput Gaussian process," *IEEE Trans. Autom. Sci. Eng.*, vol. 17, no. 1, pp. 261–272, Jan. 2020.

[18] Y. Ding, W. Zhang, X. Zhou, Q. Liao, Q. Luo, and L. M. Ni, "FraudTrip: Taxi fraudulent trip detection from corresponding trajectories," *IEEE Internet Things J.*, vol. 8, no. 16, pp. 12505–12517, Aug. 2021.

[19] Z. Qiao, L. Zhao, L. Gu, X. Jiang, R. Li, and L. Ge, "Research on abnormal pedestrian trajectory detection of dynamic crowds in public scenarios," *IEEE Sensors J.*, vol. 21, no. 20, pp. 23046–23054, Oct. 2021.

[20] N. Li, F. Chang, and C. Liu, "Spatial-temporal cascade autoencoder for video anomaly detection in crowded scenes," *IEEE Trans. Multimedia*, vol. 23, pp. 203–215, 2021.

[21] V. Mothukuri, P. Khare, R. M. Parizi, S. Pouriyeh, A. Dehghantanha, and G. Srivastava, "Federated-learning-based anomaly detection for IoT security attacks," *IEEE Internet Things J.*, vol. 9, no. 4, pp. 2545–2554, Feb. 2022.

[22] D. Połap, G. Srivastava, J. C. W. Lin, and M. Woźniak, "Federated learning model with augmentation and samples exchange mechanism," in *Proc. Int. Conf. Artif. Intell. Soft Comput.* Cham, Switzerland: Springer, 2021, pp. 214–223.

[23] U. Ahmed, G. Srivastava, Y. Djenouri, and J. C.-W. Lin, "Knowledge graph based trajectory outlier detection in sustainable smart cities," *Sustain. Cities Soc.*, vol. 78, Mar. 2022, Art. no. 103580.

[24] A. Belhadi, Y. Djenouri, G. Srivastava, D. Djenouri, J. C.-W. Lin, and G. Fortino, "Deep learning for pedestrian collective behavior analysis in smart cities: A model of group trajectory outlier detection," *Inf. Fusion*, vol. 65, pp. 13–20, Jan. 2021.

[25] Q. Chao, Z. Deng, J. Ren, Q. Ye, and X. Jin, "Realistic data-driven traffic flow animation using texture synthesis," *IEEE Trans. Vis. Comput. Graphics*, vol. 24, no. 2, pp. 1167–1178, Feb. 2018.

[26] J. Zhang, Q. Hu, J. Li, and M. Ai, "Learning from GPS trajectories of floating car for CNN-based urban road extraction with high-resolution satellite imagery," *IEEE Trans. Geosci. Remote Sens.*, vol. 59, no. 3, pp. 1836–1847, Mar. 2021.

Xiaoding Wang received the Ph.D. degree from the College of Mathematics and Informatics, Fujian Normal University, Fuzhou, China, in 2016. He is currently an Associate Professor with the College of Computer and Cyber Security, Fujian Normal University. His main research interests include network optimization and fault tolerance.

Wenxin Liu received the bachelor's degree in information security from the Xi'an University of Posts and Telecommunications, China, in 2019. He is currently pursuing the master's degree with the College of Computer and Cyber Security, Fujian Normal University. His research interests include deep learning, cyber security, and blockchain.

Hui Lin received the Ph.D. degree in computing system architecture from the College of Computer Science, Xidian University, China, in 2013. He is currently a Professor with the College of Computer and Cyber Security, Fujian Normal University, Fuzhou, China. He is also a M.E. Supervisor with the College of Computer and Cyber Security, Fujian Normal University. He has published more than 50 papers in international journals and conferences. His research interests include mobile cloud computing systems, blockchain, and network security.

Jia Hu received the B.Eng. and M.Eng. degrees in electronic engineering from the Huazhong University of Science and Technology, Wuhan, China, in 2004 and 2006, respectively, and the Ph.D. degree in computer science from the University of Bradford, U.K., in 2010. He is currently a Senior Lecturer in computer science at the University of Exeter. His research interests include edge-cloud computing, resource optimization, applied machine learning, and network security. He has published over 90 research papers within these areas in prestigious international journals and reputable international conferences. He has received the Best Paper Awards at IEEE SOSE 2016 and IUCC 2014. He has served as the General Co-Chair for IEEE CIT 2015 and IUCC 2021, and the Program Co-Chair for the IEEE ISPA 2020, ScalCom 2019, SmartCity 2018, CYBCONF 2017, and EAI SmartGIFT 2016. He serves on the Editorial Board of *Computers and Electrical Engineering* (Elsevier) and has guest-edited many special issues on major international journals, such as the IEEE INTERNET OF THINGS JOURNAL, *Computer Networks*, and *Ad Hoc Networks*.

Kuljeet Kaur (Member, IEEE) received the B.Tech. degree in computer science and engineering from Punjab Technical University, Jalandhar, India, in 2011, and the M.E. degree in information security and the Ph.D. degree in computer science and engineering from the Thapar Institute of Engineering and Technology (Deemed to be University), Patiala, India, in 2015 and 2018, respectively. She worked as a NSERC Postdoctoral Research Fellow at the École de Technologie Supérieure (ÉTS), Université du Québec, Montreal, QC, Canada, from 2018 to 2020. She is currently working as an Assistant Professor with the Electrical Engineering Department, ÉTS, and a Visiting Researcher with the School of Computer Science and Engineering (SCSE), Nanyang Technological University (NTU), Singapore. She has secured several research articles in top-tier journals, such as IEEE WIRELESS COMMUNICATIONS, IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, IEEE TRANSACTIONS ON CLOUD COMPUTING, IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, IEEE TRANSACTIONS ON MULTIMEDIA, IEEE TRANSACTIONS ON SMART GRID, IEEE SYSTEMS JOURNAL, IEEE INTERNET OF THINGS JOURNAL, *IEEE Communications Magazine*, IEEE WIRELESS COMMUNICATIONS, *IEEE Network*, IEEE TRANSACTIONS ON POWER SYSTEMS, *FGCS*, *JPDC*, and *PPNA* (Springer), and various international conferences, including IEEE GLOBECOM, IEEE ICC, IEEE PES GM, IEEE WCNC, IEEE INFOCOM Workshops, ACM MobiCom Workshops, and ACM MobiHoc Workshops. Her main research interests include cloud computing, energy efficiency, smart grid, frequency support, and vehicle-to-grid. During her Ph.D., she received two prestigious fellowships, i.e., INSPIRE Fellowship from the Department of Science and Technology, India, in 2015, and a Research Scholarship from Tata Consultancy Services (TCS) (2016–2018). She also received the IEEE ICC Best Paper Award at Kansas City, MO, USA, in 2018; the 2019 Best Research Paper Award from the Thapar Institute of Engineering and Technology; and the 2020 IEEE SYSTEMS JOURNAL Best Paper Award. She serves as an Associate Editor for *Security and Privacy* (SPY) (Wiley), *Journal of Information Processing Systems* (JIPS), and *Human-Centric Computing and Information Sciences* (HCIS) (Springer), and a Guest Editor for Special Issues in the IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS and IEEE OPEN JOURNAL OF THE COMPUTER SOCIETY. She is a Website Co-Chair of the N2Women Community. She also serves as the Vice-Chair for the IEEE Montreal Young Professionals Affinity Group. She has also been a TPC Co-Chair of the IEEE Infocom 2020 and ACM MobiCom 2020 Workshops on DroneCom. She is a member of the IEEE Communications Society, IEEE Computer, IEEE Women in Engineering, IEEE Software Defined Networks Community, IEEE Smart Grid Community, ACM, and IAENG.

M. Shamim Hossain (Senior Member, IEEE) received the Ph.D. degree in electrical and computer engineering from the University of Ottawa, Ottawa, ON, Canada, in 2009. He is currently a Professor with the Department of Software Engineering, College of Computer and Information Sciences, King Saud University, Riyadh, Saudi Arabia. He is also an Adjunct Professor with the School of Electrical Engineering and Computer Science, University of Ottawa. He has authored or coauthored more than 335 publications. His research interests include cloud networking, smart environment (smart city, smart health), AI, deep learning, edge computing, the Internet of Things (IoT), multimedia for health care, and multimedia big data. He is a Distinguished Member of the ACM. He was a recipient of a number of awards, including the Best Conference Paper Award, the 2016 *ACM Transactions on Multimedia Computing*, Communications and Applications (TOMM) Nicolas D. Georganas Best Paper Award, and the 2019 King Saud University Scientific Excellence Award (Research Quality). He is the Chair of the IEEE Special Interest Group on Artificial Intelligence (AI) for Health with IEEE ComSoc eHealth Technical Committee. He is also the Co-Chair of the 2nd IEEE GLOBECOM 2022 Workshop on Edge-AI and IoT for Connected Health. He is the Technical Program Co-Chair of ACM Multimedia 2023. He is also the Chair of the Saudi Arabia Section of the Instrumentation and Measurement Society Chapter. He is on the Editorial Board of the IEEE TRANSACTIONS ON INSTRUMENTATION AND MEASUREMENT, IEEE TRANSACTIONS ON MULTIMEDIA, *ACM Transactions on Multimedia Computing, Communications, and Applications* (TOMM), IEEE MULTIMEDIA, *IEEE Network*, IEEE WIRELESS COMMUNICATIONS, IEEE ACCESS, and *Journal of Network and Computer Applications* (Elsevier). He has served as a Lead Guest Editor for more than two dozen of Special Issues (SIs), including *ACM Transactions on Multimedia Computing, Communications, and Applications* (TOMM), *ACM Transactions on Internet Technology*, *IEEE Communications Magazine*, *IEEE Network*, IEEE TRANSACTIONS ON INFORMATION TECHNOLOGY IN BIOMEDICINE (currently JBHI), IEEE TRANSACTIONS ON CLOUD COMPUTING, and *Future Generation Computer Systems* (Elsevier). He is an IEEE Distinguished Lecturer (DL).