Federated Visualization: A Privacy-preserving Strategy for Aggregated Visual Query

Wei Chen, Yating Wei, Zhiyong Wang, Shuyue Zhou, Bingru Lin, and Zhiguang Zhou

Abstract—We present a novel privacy preservation strategy for aggregated visual query of decentralized data. The key idea is to imitate the flowchart of the federated learning framework, and reformulate the visualization process within a federated infrastructure. The federation of visualization is fulfilled by leveraging a shared global module that composes the encrypted externalizations of transformed visual features of data pieces in local modules. We design two implementations of federated visualization: a *prediction-based* scheme, and a *query-based* scheme. We demonstrate the effectiveness of our approach with a set of visual forms, and verify its robustness with evaluations. We report the value of federated visualization in real scenarios with an expert review.

Index Terms—Privacy-preserving visualization, federated visualization, decentralized visualization

✦

1 INTRODUCTION

In big data era, a wide array of data are being generated all the time and scattered over different data holders. It is a significant task to closely connect data holders and conduct collaborative data analysis for deeper insights and comprehensive conclusions. For example, the combination disease materials and cases collected in different locations and a medical institution is quite important for the analysis of infectious diseases [1], [2]. Similarly, urban data analysis demands the integration of mobility information acquired from subway, taxis and automobiles [3], [4].

In visualization community, two kinds of methods are commonly used for collaborative data analysis including data-intensive visualization and distributed visualization. Conventional client/server based visualization and web-based visualization take a data-intensive mode, in which datasets are assembled, processed and visualized in a main server [5], [6]. Alternatively, distributed visualization [7] employs a decentralized mode, in which datasets and tasks are divided into pieces over various clients, and required information can be transmitted among clients.

In the both modes, raw datasets and their processed results are allowed to be transmitted among clients, and users can easily

- W. Chen is with The State Key Lab of CAD & CG, Zhejiang University, Hangzhou, Zhejiang 310058, China.
  E-mail: {chenvis} @zju.edu.cn

- Y. Wei is with The State Key Lab of CAD & CG, Zhejiang University, Hangzhou, Zhejiang 310058, China; and Zhejiang Metals And Materials Co., Hangzhou, Zhejiang 310003, China.
  E-mail: {weiyating} @zju.edu.cn

- Z. Wang is with the Tencent, Guangzhou 510630, China.
  E-mail: {zerowangzy} @zju.edu.cn

- S. Zhou, and B. Lin are with the Alibaba Group, Hangzhou, Zhejiang 310058, China.
  E-mail: {tangmao.zsy, bingru.lbr} @alibaba-inc.com

- Z. Zhou is with Hangzhou Dianzi University, Hangzhou, Zhejiang 310018, China.
  E-mail: {zhgzhou1983} @163.com

- Wei Chen is the corresponding author.

aggregate and analyze the datasets at different stages. However, there is a great risk of privacy leakage in the entire course of data processing. For example, in the data-intensive mode, users can directly get the dataset from a client on the server side. In the distributed mode, users can reversely infer the data information of a client through additional data information [8]. Thus, it is urgent to provide a feasible multi-source data visualization method without privacy leakage.

Privacy protection is a classic proposition in the field of visualization. One recent trend in building big data infrastructures is the privacy awareness, as witnessed by numerous literature on security and privacy [9], [10]. Though privacy-aware visualization has been explored in the visualization community, existing works emphasize on protecting data leakage within a centralized visualization process [9], [11]. There are still a few challenges for tackling privacy issue in the decentralized visualization: C1. A conventional visualization pipeline consists of multiple steps, including data processing, transformation, visual mapping, and user interaction. Data leakage can take place in each step in decentralized mode. Data encryption should be thoroughly incorporated as a necessary component. C2. For the reason of privacy protection, data in local modules should be kept locally, and only desensitized information can be transmitted to the global module. Thus, to generate faithful visualization based on composed information in global module is quite different from that in centralized mode. C3. It is important to evaluate the validity and usability of decentralized visualization in the protection of privacy and collective analysis based on multi-source datasets. Multiple perspectives like encryption, privacy, and effectiveness should be considered different from centralized visualization.

In the field of data mining, facing the challenges of data privacy in distributed machine learning, federated learning employs a shared global model to federate the learned local models that run only in individual clients, and uses a variety of encryption schemes in the data transmission process [10-12]. Inspired by the idea of federating learned features rather than raw data, we design a federated aggregation visualization strategy, which divides the tasks of data transformation and visual mapping into pieces in clients (local modules) and then composes the secured results in a server (a shared global module). We propose a framework for

privacy-preserving decentralized visualization, in which federating learned features are integrated into the conventional visualization pipeline [12]. A data encryption scheme is employed to transmit data between the server and clients. To localize the underlying data and visualization tasks, we design a two-stage pipeline: prior to the composition of encrypted visual features or parameters in the server, each client locally performs data transformations and visual encodings with its associated data(C1). Specifically, we implement two federated aggregation visualization schemes for different data analysis scenarios: a *query-based* scheme and a *prediction-based* scheme. The *query-based* scheme computes encrypted and specified range of visual features locally and composes them globally, through which users can quickly obtain target visualization in a short response time. The *prediction-based* scheme builds a prediction model to encode visual features computed from local data, and decode them in the global module. It can realize the analysis of all data scenarios, of course requires more time to train the model to fit the data distribution of each client (C2). Moreover, we develop a federated aggregation visualization framework integrating different federated visualization schemes, a rich set of visual cues and interactions, enabling users to evaluate the effectiveness and practicality of our federated visualization strategy in the protection of privacy and collaborative analysis of multi-source data (C3).

In summary, the main contributions of our work are:
- a novel federated visualization framework for visualizing aggregated visual query of decentralized data. To our best knowledge, our approach is the first attempt to tackle data privacy issues in a decentralized visualization framework.
- two implementation schemes for different data analysis scenarios. They are integrated into the proposed framework.
- evaluation and verification based on real world data. Experiments and cases demonstrate that effective visual analysis can be conducted while preserving privacy.

The rest of this paper is organized as follows. Section 2 reviews the related work. Section 3 explains our new strategy. Implementations and visual exploration are elaborated in Section 4. Section 5 presents the evaluations. We discuss the limitations and future work in Section 6 and conclude this paper in Section 7.

2 RELATED WORK

2.1 Privacy-preserving Visualization

Privacy is the right of individuals to take complete control of their information and decide when, how, and to what extent this information is shared with others [13]. Visualization is regarded as an effective means to make the data or data features easily recognizable and interpretable. Therefore, privacy issues of visualization exist not only in data processing but also visualization itself. In the field of privacy-preserving data processing, two types of privacy models, syntactic anonymity [14], [15], [16], [17] and differential privacy [18], are commonly used to address privacy issues. The former one is mainly used for privacy-preserving data publishing, the latter is designed to anonymize query responses. Pioneered works on privacy-preserving visualization [11] generally leverage established privacy preservation schemes like *k*-anonymity [14], *l*-diversity [15], *t*-closeness [16] to protect information leakage in visualizations. For instance, syntactic anonymization is employed to protect the information exposed in parallel coordinates [11]. A privacy-preserving diversity method (ppDIV) [3] is presented to avoid disclosure of location privacy from trajectory heatmap.

Distinctive visual interfaces are designed to depict and reduce the leakage risk in visualizing event sequence datasets [19], [20], and tabular data [9]. In general, there is a trade-off between the privacy gain and loss of utility. It has demonstrated to be favorable to support visual understanding of the quantitative relationship between privacy parameters and vulnerable visualization configurations [21].

Note that, above-mentioned works do not consider the disclosure of privacy in data transmission process, and are naturally not suitable for decentralized visualization.

2.2 Distributed Visualization

Distributed visualization [7], [22] increases the scalability of visualization for data-intensive or computation-intensive tasks. A distributed environment is proposed for exploring correlations of large-scale simulation datasets. Well-designed data structures can be used to improve the performance of distributed visualization, like the PSH [23] and quadtree [24]. GPU-based parallel computing can further improve performance [25]. Likewise, the runtime efficiency of graph sampling [26] and sparsification [27] can be benefited from distributed computing. Note that these studies emphasize on the performance issues. There is little effort made on data privacy in distributed visualization. Saha et al. [2] introduce decentralized data stochastic neighbor embedding (dSNE) to enable embedding and visualization of sensitive neuroimaging data. Similarly, a decentralized brain imaging data analysis is proposed with new data processing and visualization algorithms [1].

2.3 Federated Learning

The fundamental idea of federated learning (FL) [28] is to learn an integrated model with data distributed on clients. It can balance performance and communication efficiency while preventing leakage of sensitive data. A large number of studies have been made on the usability, scalability, and performance of FL [29], [30]. For instance, an optimized federated learning strategy is proposed to train a high-quality centralized model [31]. By investigating enhanced privacy protection algorithms, different levels of privacy protection can be achieved in FL at a minor loss in model performance [32], [33], [34]. A recent trend is to incorporate FL within a variety of application scenarios [35], [36], [37], [38]. In these application settings, FL extracts the significant features from each client's data using deep learning algorithms, such as various classifiers [39], [40]. The generalized global model is then generated based on the retrieved features from each client in order to perform the analytic task, such as visual object detection [41] and network traffic anomaly detection [42]. To train high-quality FL models, client data heterogeneity is one of the primary considerations. Visually comparing the behaviors of the global federated model and the locally trained model can reveal data heterogeneity [43]. Concerning the distribution of training data, federal learning approaches can be classified into three categories: horizontal federated learning (HFL), vertical federated learning (VFL), and Federated Transfer Learning (FTL) [44]. In this paper, we focus on HFL, which can be applied in scenarios where datasets mastered by clients are collected respectively but share the same properties. Informed by the application of federated learning, we present a federated aggregation visualization strategy.

3 FEDERATED VISUALIZATION

The goal of federated visualization is to protect privacy in a decentralized visualization framework. Suppose that a set of datasets $\mathbf{D} =$
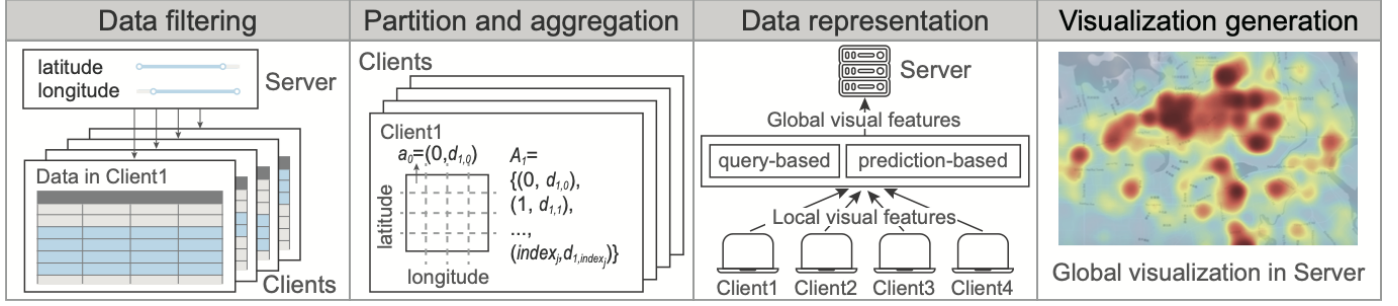
Fig. 1. The pipeline for federated visualization consists of four main stages.

$\{D_1, D_2, D_3, ..., D_N\}$, owned by clients $\mathbf{C} = \{C_1, C_2, C_3, ..., C_N\}$, respectively. Assume that V_i is the visualization of D_i, and $\mathbf{V}$ is the visualization of $\mathbf{D}$. Without loss of generality, V_i and $\mathbf{V}$ share the same visual transformations and mappings, resulting in a set of visual features, denoted as $\mathbf{V} = \{VF_1, VF_2, ..., VF_M\}$. Here, $VF_i = \{vf_{i1}, vf_{i2}, ..., vf_{iM}\}$ is a vector of visual features, such as position, color, size, and shape. $\mathbf{V}$ represents the global visual features of $\mathbf{D}$. In the conventional parallel visualization, $\mathbf{D}$ is collected and processed globally in a server $\mathbf{S}$, exposing a risk of privacy leakage. In this paper, we only consider the scenario that the visual features of each client have the same dimensions, which refers to the situation of **HFL** [44].

We propose a two-stage federation strategy based on the flowchart of *horizontal federated learning*. Datasets are stored and processed locally in each client C_i. C_i only transmits encrypted parameters P_i which represents visual features and cannot be used to recover the original data. P_i acts as the messenger of the original data D_i and $\mathbf{V}$, to avoid direct exposure of the raw data. The definition and construction of P_i varies with different federation schemes (see Section 3.2).

3.1 Pipeline

The pipeline consists of four main stages, as shown in Figure 1:

1) **Data filtering**. First, the data scope E_i associated with D_i is specified by analysts, e.g., data in a specific latitude and longitude range, or data in a specific time period. It can be defined uniformly for all clients or be specified interactively on the visual interface during the exploration process.

2) **Data partitioning and aggregation**. For each client, its data is partitioned into small pieces uniformly. The resolution of the partition can be predefined or interactively specified subject to the employed visual forms. For instance, creating a heatmap requires dividing the data over a 2D grid. Similarly, generating a histogram of traffic flow in one week needs to define the granularity along the time axis.

   Then, data aggregation is performed over each binned range of the partition. The aggregated values are mapped into visual features, forming a visual feature set A_i. Each element a_j of A_i is a key-value pair, namely, $a_j = (index_j, d_{i,index_j})$. Here, $index_j$ denotes the index, and d is the feature values of $index_j$. This process is performed on each client, resulting in visual features with identical dimensions.

3) **Data representation**. This process requires analysts to encode and encrypt visual features in each client and utilize them in the server. For that, we design two implementations, which are described in Section 3.2.

4) **Visualization generation**. Based on the encrypted visual features from local clients, the server composes a set of global visual features and generates a visualization. This process requires an additional layer of privacy preservation for the generated visualization in to prevent attackers from re-identifying small sample size data via the visualization. Section 3.3 describes the ways of visualization creation associated with two representations introduced in Section 3.2.

3.2 Federated Representation

In the third stage, it is crucial that the visual features of each client are not exposed during the transmission process. We solve this issue by transmitting encrypted parameters representing visual features. Specifically, two implementations are designed:

- *Query-based*, which encodes local visual features using secure aggregation techniques and decodes them on the sever;
- *Prediction-based*, which employs federated learning to train a prediction model on each client and predicts the output on the server using all parameters of local prediction models.
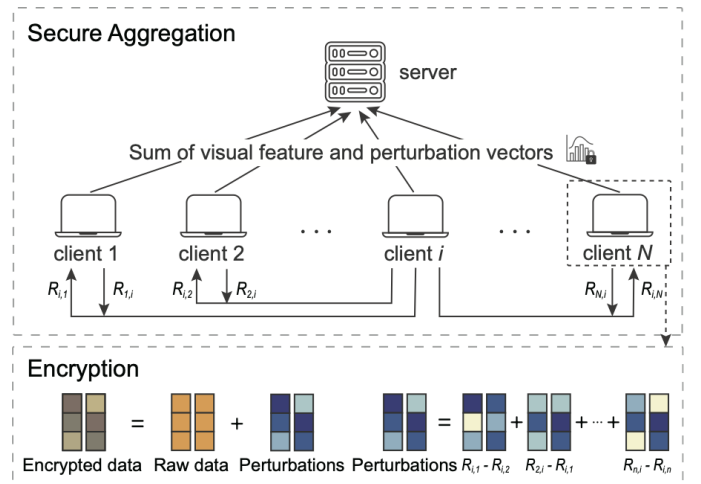
3.2.1 The query-based scheme

Fig. 2. The flowchart of the *query-based* scheme.

The *query-based* scheme consists of three steps:

[1] Sampling random vectors. Each pair of clients first prepares a random vector for each other. That is, each client C_i locally samples a random vector $R_{i,j}, j \in [1, N] \wedge i \neq j$ for each other client C_j. Specifically, $R_{i,j}$ and $R_{j,i}$ are a one-to-one pair. For

example, $R_{1,3}$ and $R_{3,1}$ form the random vectors prepared by C_1 and C_3 for each other (Figure 2).

[2] Exchanging random vectors and computing perturbations. Client C_i and C_j exchange $R_{i,j}$ and $R_{j,i}$ over their secure channels. To ensure transmission security, perturbations $P_{i,j} = R_{i,j} - R_{j,i}, i \neq j$ are computed. The sum of visual feature and perturbation vectors is sent to the server: $D\_upload_i = VF_i + \sum_{j=1}^{N} P_{i,j}$.

[3] Computing global visual features in the server. The server receives the perturbed vectors $D\_upload_i, i \in [1, N]$ uploaded by clients, and sums them:

$$D\_sum = \sum_{i=1}^{N} D\_upload_i = \sum_{i=1}^{N} VF_i + \sum_{i=1}^{N}\sum_{j=1}^{N} R_{i,j} - \sum_{i=1}^{N}\sum_{j=1}^{N} R_{j,i} = \sum_{i=1}^{N} D_i$$

The result D_sum is guaranteed to be accurate visual features because the paired perturbations in D_upload_i are neutralized. And the values of each client will not be inferred.

3.2.2 The prediction-based scheme

Encoding visual features can be accomplished by precomputing a representation with the *prediction-based* approaches. Conventional solutions include data fitting like logic regression, hashing, and neural network approaches. We choose to use neural network-based methods and mimic the federated learning framework where all clients contribute to training a shared global model that represents global data features. Below, we introduce our scheme based on neural network-based models.

We leverage a fully connected deep network [45], as shown in Figure 3 (a). It consists of an embedding layer that converts the input data into vectors to improve the efficiency of model training, and five fully connected layers. The number of neurons in each layer is 128. To enable the federation of the prediction models, we design an adapted NN model, which consists of a global part and local parts (See Figure 3 (b)). The server keeps the global part, while each client keeps a local part. We consider the visual feature set A_i as the local model training set of C_i, where $index_j$ is used as the model input and $d_{i,index_j}$ is used as the label data, that is, the model output. We use the loss function defined as $\sum_i (d_{i,index_j} - \hat{d}_{i,index_j})^2$, where i is the index of the underlying data piece, $\hat{d}_{i,index_j}$ denotes the value of the data predicted by the global model. We use the quadratic cost so that $d_{i,index_j}$ will be close to the average of $\hat{d}_{i,index_j}$ over all clients.

The training process consists of three steps:

1 Initialization. The server S initializes a global neural network model M_fed. Each client keeps a copy of the initialized model from the server. The server sends encrypted initial parameters of the global NN model to each client.

2 Local training. Each client decodes the parameters sent from the server, and uses them to update the local models. Then, the local NN model is iteratively trained for several rounds with A_i as the training set, yielding updated parameters of the local NN model. The parameters are encrypted and sent back to the server.

3 Federated averaging. The server performs a federated averaging [28] over the set of encrypted parameters(in the form of $P_i(t)$, where t represents one round, including the embedding matrix and weight matrix) from all clients, and computes updated global parameters, $P(t)$: $P(t) = \frac{1}{N}\sum_{i=1}^{N} P_i(t)$. The parameters are then encrypted and sent to each client.

The 2nd and 3rd steps are iteratively performed until the loss function converges, or says, the values of two consecutive iter-
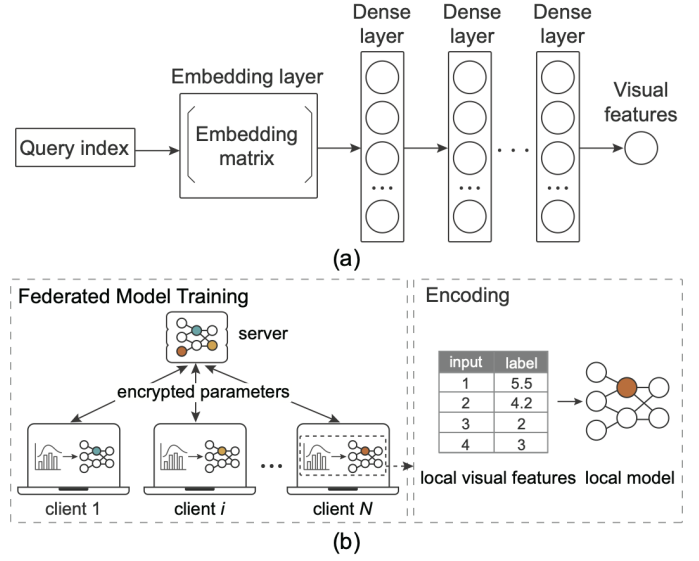

(a)

(b)

Fig. 3. An illustration of the *prediction-based* scheme. (a) The network structure of the employed NN model. (b) The training and prediction processes.

ations are adequately close. The trained NN model parameters are stored on the server for reuse.

3.3 Federated Composition

For a visual form to be created, relevant visual features are generated in each client. The encryption of model parameters or values is transmitted to the backend server. Visual features are reconstructed with respect to the employed scheme in the representation stage (Section 3.2).
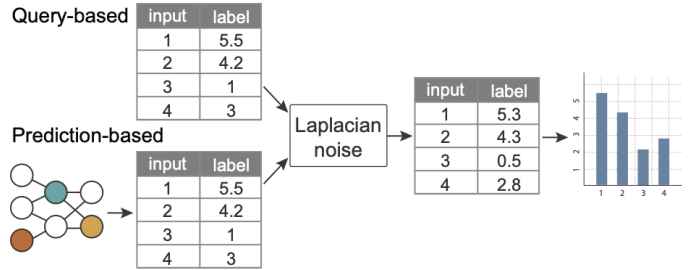

Fig. 4. The process of federated composition with two schemes: the *query-based* scheme and the *prediction-based* scheme. In both schemes, Laplacian noise is added to the global visual features to prevent attackers from inferring individuals through global visual features. More noise will be added to smaller visual features.

- For the *query-based* scheme, the server directly extracts accurate visual feature values.
- For the *prediction-based* scheme, the index $index_j$ is used as the input of the trained global model M_fed, and the output d_j can be expressed as:

$$d_j = \sum_{i=1}^{N} d_{i,index_j}/N$$

It is approximately the average of the aggregated values of each client within the data range $index_j$. Therefore, visual features of the global data on $index_j$ are $N \times d_j$. In this way, we can get all the visual features by feeding all the indices into the global model M_fed.
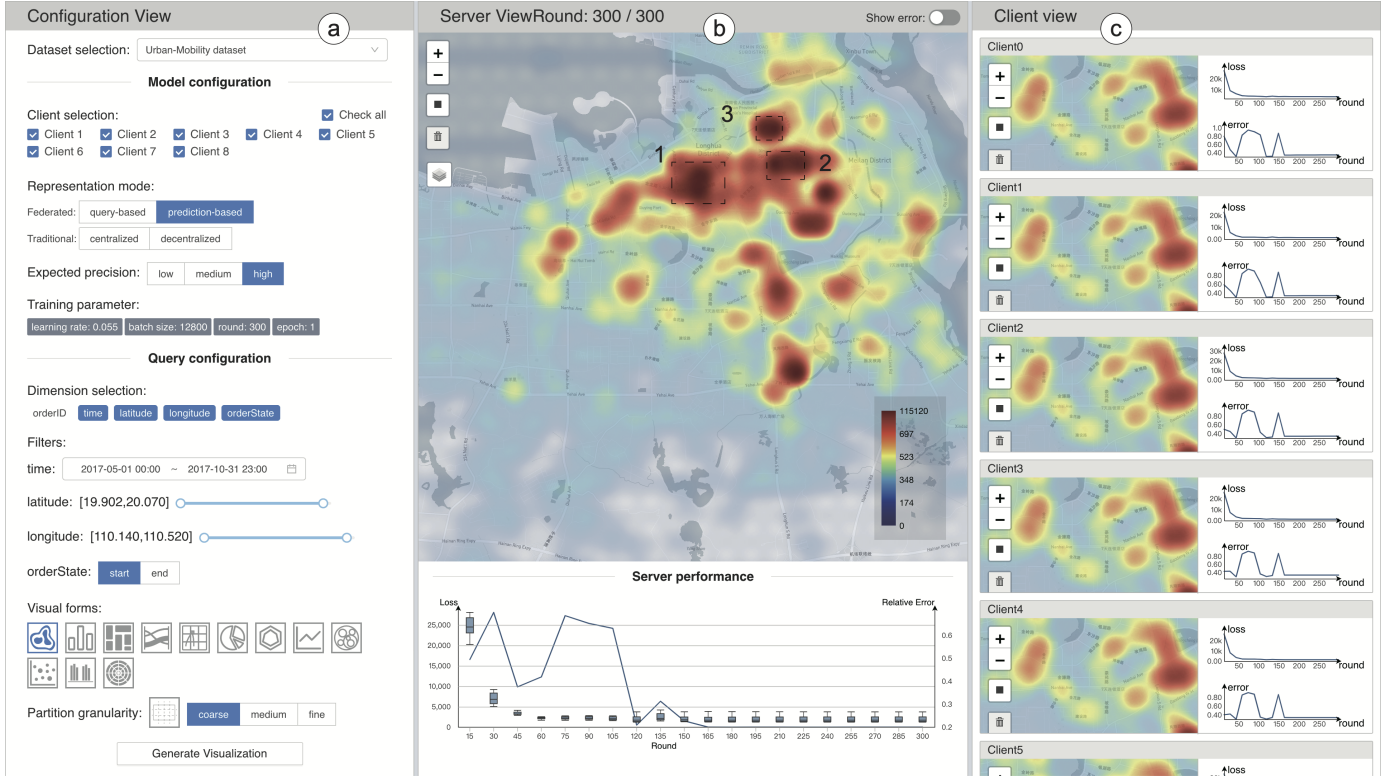
Fig. 5. Demonstration of our approach with the Urban-Mobility dataset. Here, one server and eight clients are employed. The *prediction-based* scheme is used to fulfill the federation of visualization. (a) The configuration view allows users to configure the relevant parameters of the federated scheme and query conditions. (b) The server view displays the global visualization result and the dynamic performance of the server. (c) The client view shows the local visualization and its performance.

In order to prevent the reconstructed global visual feature values from leaking privacy, we employ differential privacy [46] before visualization composition. When the visual feature value is small, it is easy to re-identify individuals [14]. Thus, we add more noise to visual features with relatively small values. As shown in Figure 4, after reconstructing the global visual features, we use the Laplace mechanism to add the random noise into the visual features. Then, the visual feature values with noise can be used for federated visualization to achieve privacy protection.

4 VISUAL INTERFACE

We design and develop a prototype system for our framework.

4.1 Interface

The visual interface (Figure 5) consists of three main modules: configuration view, server view, and client view. The configuration view includes model and query configuration. In the model configuration module, the user specifies the clients that will participate in the federated visualization, and then selects the representation scheme to be applied. The representation modes are divided into two categories for comparison. The federated representation mode is the strategy we propose in this paper, including the query-based and prediction-based schemes, which are all decentralized visualization methods. The traditional representation mode does not perform data encryption operations, directly merges data in centralized mode, or distributes computing and then directly merges in decentralized mode. If the *prediction-based* scheme is used, the user must also specify the expected precision, which indirectly determines the

model training parameters. In the query configuration module, the user selects the dimension to explore and specifies the data range. Several commonly-used visual forms are listed. When a visual form is selected, the corresponding data partition will be displayed. The user must specify the data partitioning granularity. Once all configuration items have been completed, the user can obtain the federated visualization results. The server view shows the global visualization and the performance of the server. To observe the precision of the results, the user can either view the error in the performance line chart or switch to the error chart. To help users clearly comprehend the federated framework, the results and performance of each client using its own local data for visualization are displayed in the client view. Users can compare local and global results with ease.

4.2 Federated chart generation

Below, we show the creation of a variety of aggregation-based visualizations, ranging from structured tabular data to hierarchical datasets. Both the *query-based* scheme and the *prediction-based* scheme can be leveraged to get global visual feature values for visualization creation. The flexibility of federated visualization is highlighted in each example.

Histogram. To create a histogram, it is necessary to determine the number and height of bars. Suppose the target histogram has seven bars, which represent the seven days of a week, and each bar's height incicates the daily traffic volume. To generate it, each client's local data is divided into seven pieces, for each of which the overall traffic volume is computed. Thus, each client obtains a local visual feature set for visual mapping. To get the global

visual features of the entire dataset, on one hand, we can use the *query-based* scheme to directly encrypt and merge visual features of each client; on the other hand, the *prediction-based* scheme can be used to fit the global visual features where the local visual feature set is used as the local training set. To further explore the finer granularity of the information, we create a stacked histogram. The underlying data of each bar is divided and computed to obtain a new visual feature set for visual mapping of the stacked histogram.

In general, the method of creating a histogram can be applied to generating other chart types, such as the line chart, pie chart, violin plot, area chart, and radar chart.

Heatmap. The heatmap in Figure 5 consists of 15960 (190×84) grids divided by uniform longitude and latitude. Each grid cell has an index and a value. The accumulated density in each grid cell is encoded by hue, which represents the number of records in the corresponding geographic area. On each client, a heatmap is calculated based on local data. Those heatmaps, reflecting the distributions of datasets on each client, have the same cell index. Our goal is to get an overall heatmap that reflects the distribution of all clients' datasets without leaking privacy.

Similarly, to create an ODMap (Origin-Destination flow map), the local data is partitioned according to the latitude and longitude of the map. In each resultant part, the partition is performed along the latitude and longitude of the destinations. Then, the traffic flow from the origins to the destinations is computed, resulting in a four-dimensional division. When the division is relatively dense, the *predictive-based* scheme is more time-consuming than the *query-based* one due to the necessity to train a large number of visual feature values.

Sankey diagram. Sankey diagrams are a specific type of node-link diagram. Several entities are represented by rectangles or text, and their links are represented with arrows or arcs whose widths are proportional to their flow quantities. To create a sankey diagram, flow quantities from different clients should be integrated without merging data. To solve this issue, each client defines data statistics rules according to the visual analysis task and divides and counts the local data according to the rules. For example, when examining population migration between countries, each client divides and counts *in* and *out* fields based on different countries. For final visualization, this processed data is then encrypted and merged.

Squarified Treemaps. Federated visualization is capable of creating recursive layouts, such as the treemap, sunburst, and circle packing diagram. The data structure of hierarchical data (where the data is organized into a tree structure) is more complex than that of tabular data. Without loss of generality, the tree structures of all clients are assumed to be identical. For example, in the case of aggregating street sign-in information from various regions of the country from different clients, the hierarchy of the geographic locations of the clients is the same. Thus, each client merely needs to count the numbers of leaf nodes and provide their encryption key in order to craft a treemap, after which the server can summarize and present the treemap.

4.3 Federated Visual Analysis

Visual exploration with federated visualization forms a seamless composition of multiple client and server steps. First, the visualization configurations of federated visualization are determined in the front-end. Users can specify the participation, the representation mode, the data range, and the visual form in the configuration view. After the user selects the dimension and visual form, the

system will automatically complete the visual mapping. Second, the configurations are sent to the server. The server determines the scheme based on the chosen representation mode and sends the configurations to all clients. Third, clients process the local data according to the representation mode and send the results back to the server. Fourth, the front-end gets visual feature values from the server and creates the visual forms.

Several basic interactions, such as selection, navigation, and filtering, are supported. When the user clicks the "Generate Visualization" button, the information transmission between the server and clients will be triggered. For the *query-based* scheme, the dataset stored on each client is queried. For the *prediction-based* scheme, the model needs to be re-trained, and related parameters are updated for each new query. Pre-computing results of all or parts of model configurations can eliminate the workload of model re-training in run-time visual queries, as was done in previous works [47].

5 EVALUATION

We implement a web-based prototype system. The source code of our system is available at: https://github.com/ZeroWangZY/fed-vis. The back-end is written in Python. The front-end visualization is implemented with a combination of HTML5, JavaScript, and D3.js. SocketIO is used to communicate between clients and the server. TensorFlow is used to implement our deep learning model. All clients are simulated on a single machine with eight simulation nodes, which has an i7-8700 processor and a GTX 1660Ti GPU.

5.1 Quantitative evaluation

The quantitative evaluation compares our two schemes with the centralized counterpart with three measures: performance, accuracy, and error chart.

5.1.1 Performance

The response time includes time spent on data filtering, data partition and aggregation, data representation and visualization generation. The difference between federated visualization and traditional visualization methods lies in the data representation phase. The timing measurement indicates the impact of factors such as the granularity of data partitioning, the number of training rounds, and the number of clients.

Query-based scheme. Compared with traditional centralized visualization, extra time is spent on data encryption. It mainly includes three parts: generating random vectors, exchanging random vectors, encrypting and decrypting data. We assume that both the number of clients and the granularity of data partitioning affect the response time.

Number of clients: The number of clients is set to 3, 5, 8. The response time presents an upward trend as the number of clients increases(Table 1). This indicates that the response time increases as the number of participating clients gradually increases. Clearly, the rate of response time increase depends on the underlying encryption mechanism. The time required to exchange random vectors dominates the computation. This is because its time complexity is $O(n^2)$.

Granularity of data partitioning: Different chart types have different granularities, or the number of visual features, resulting in varied response times (Table 1). The response time of a heatmap is the longest, followed by those of a treemap and histogram. This

TABLE 1
Quantitative results of the time measurement for heatmap, histogram, i.i.d. treemap and non-i.i.d. treemap using the *prediction-based* scheme and the *query-based* scheme under different settings of the number of client and training round. The unit of time is seconds.

#client		3			5			8		
#round		50	150	300	50	150	300	50	150	300
Prediction-based	Heatmap(380 × 168)	17.5633	52.3755	102.8733	29.8091	87.8196	174.8193	47.6048	140.334	278.6307
	Histogram(24 × 7)	1.8203	4.7769	7.6263	2.7338	6.6951	12.6123	3.8703	10.2641	19.6864
	Treemap(6000)	2.7662	6.433	12.7318	4.4036	11.8682	20.1864	6.3223	16.3948	31.6249
Query-based	Heatmap(380 × 168)		2.2464			2.4535			2.7742	
	Histogram(24 × 7)		2.0591			2.106			2.1822	
	Treemap(6000)		2.21			2.1269			2.1946	

TABLE 2
Quantitative results of the accuracy measurement for heatmap, histogram, i.i.d. treemap and non-i.i.d. treemap using the *prediction-based* scheme under different settings of the number of client and training round. We use the RE metric to measure the accuracy of visualization, which indicates the difference between two visualizations.

#client		3			5			8		
#round		50	150	300	50	150	300	50	150	300
Prediction-based	Heatmap(380 × 168)	0.1286	0.0804	0.0821	0.1584	0.1185	0.1176	0.1783	0.1587	0.141
	Histogram(24 × 7)	0.1111	0.0261	0.0233	0.041	0.0307	0.0296	0.0458	0.0324	0.0286
	Treemap i.i.d.(6000)	0.0146	0.001	0.002	0.0025	0.0025	0.0008	0.0023	0.0025	0.0026
	Treemap non-i.i.d.(6000)	0.0109	0.0003	0.0005	0.001	0.0007	0.0006	0.0005	0.0009	0.0012
Query-based	*		0			0			0	

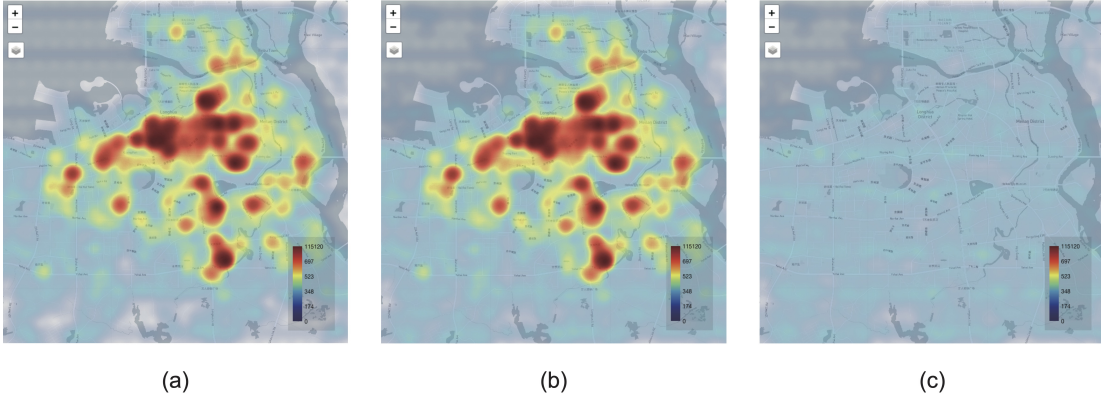(a)   (b)   (c)

Fig. 6. Applying the *prediction-based* scheme in querying a heatmap. From left to right: (a) the predicted result, (b) the exact result, (c) the difference map. To make the difference noticeable, the difference values are enlarged by 50 times.

is due to the decreasing granularity of data partitioning, which is 380 × 168, 6000, 24 × 7, respectively.

Prediction-based scheme. The time overhead for the *prediction-based* scheme lies in model training. Several factors may influence the time of model training, such as the granularity of data partitioning, the training settings, the number of clients, and the data distribution.

Granularity of data partitioning: Table 1 shows the relationship between response time and data partitioning granularity. Similar to the query-based scheme, the results indicate that as the number of visual features to be trained increases, so does the training time. Compared with the result of the query-based scheme in Table 1, the *prediction-based* scheme requires significantly more time.

Training settings: The response time presents an upward trend as the number of training rounds increases (Table 1). Meanwhile, the response time of charts with a finer granularity will be relatively longer to fit more visual feature values.

Number of clients: The response time increases proportionally with the number of clients (Table 1). As the number of participating customers increases, so does the quantity of training data, necessitating additional time for model convergence.

5.1.2 Accuracy of visualization

With the *query-based* scheme, a small amount of Laplacian noise has been added to the queried visual features, and the results are still relatively accurate. In contrast, errors occur with the *prediction-based* scheme because visual features are approximately generated. Several factors, including the granularity of data partitioning, the training settings, the number of clients, and the training data distribution, may impact the accuracy of the visualization. A measurement of accuracy is considered. We use the relative error (RE) metric to evaluate the difference between two visualizations. Suppose that a visualization contains N feature values. Federated visualization fits original N visual features $\hat{y}_1, ..., \hat{y}_N$, and returns N values $y_1, ..., y_N$. The RE of the visualization is defined as:

$$RE = \frac{\sum_{i=1}^{N} |y_i - \hat{y}_i|}{\sum_{i=1}^{N} |y_i|}$$

Training settings: RE is inversely proportional to the number of training rounds (Table 2). Consequently, as the number of training rounds rises, the global model approaches the global optimal.

Number of clients: As shown in Table 2, RE does not fluctuate significantly with the number of clients.

Granularity of data partitioning: Table 2 shows that there is no relationship between accuracy and the chart type, or data

partitioning granularity. The results of the heatmap are relatively larger than those of the other two charts. This may be because the distribution of a heatmap is uneven and there are several visual features whose value is 0.

Training data distribution: Many works [48] have studied the distribution of training data in the field of federated learning. The training data on each client can be independently identically distributed (i.i.d.) or non-i.i.d. In practice, we randomly generate i.i.d. and non-i.i.d. treemap data to simulate actual usage scenarios and analyze the impact of data distribution on response time. As shown in the Table 2, there is almost no difference in response time between two distributions, indicating that the data distribution has little impact on the accuracy of our method.

5.1.3   Error chart

We compare our results with those generated by conventional centralized visualization, and generate an error chart. For example, we generate a difference map (Figure 6) for heatmap. We use the same colormap as the heatmap to encode the absolute value of the difference. The relative error of the obtained result in Figure 6 (a) is 0.003. This indicates little difference between the result with the *prediction-based* scheme and the exact result. Both outcomes are visually identical.

5.2   Case studies

In this section, we describe how our framework enables users to achieve aggregated visual queries and use various visual forms for visual analysis while protecting data privacy. We invite three users to participate in case studies on three real-world datasets. Each dataset's records are distributed over eight clients and are non-i.i.d. across clients (i.e., they are not independent and identically distributed (i.i.d.)). The system provides four modes: traditional centralized mode, traditional decentralized mode, federated *query-based* mode and federated *prediction-based* mode. Users can switch modes according to analysis requirements.

5.2.1   Case One: The United States Cancer Statistics dataset

The United States Cancer Statistics (USCS) dataset is the official statistics on cancer incidence by region, race, sex, year, and leading cancer site. We extracted cancer incidence data from 2007 to 2017, including 222,133 data records.
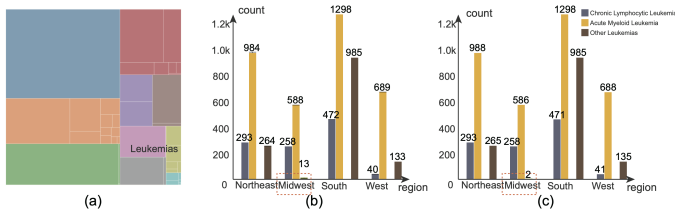

Fig. 7. The treemap of traditional desentralized mode shows that the incidence of Leukemias is relatively small (a). The histograms of the federated *query-based* mode (b) and the traditional decentralized mode (c) have a little difference. The error bars are shown in (b).

First, the user chooses the traditional decentralized mode in the configuration view. He uses a treemap to visualize the dimension "Cancer site" and observes the incidence of different cancer sites (Figure 7 (a)). He finds that the incidence of Leukemias is relatively small. Then he queries the incidence of Leukemias subcategories

in different regions and filtered by "sex = male", "race = Black or African American" and "year = 2010". The results are presented in a user-specified grouped histogram, as shown in Figure 7 (c). He notices that there are only two men in the Midwest region who have Chronic Myeloid Leukemia cancer. Such a pattern is sensitive and has a high privacy risk. The attacker is likely to infer sensitive attributes or reveal individual identities with knowledge of quasi-identifiers.

Then, he chooses the federated query-based mode to conduct the same exploration (Figure 7 (b)). He finds that even if he uses the same query conditions, the results are slightly different. This makes it difficult to re-identify raw data items. When he switches to the error chart, he observes that when the visual feature value is small, the error value is relatively large, which increases the difficulty for the attacker to re-identify. This shows that our scheme can protect privacy well.

5.2.2   Case Two: The MovieLens dataset

This dataset describes ratings from MovieLens, a movie recommendation service. It contains 1,000,208 records, including movie, user, and rating information. In order to simplify the case, we evenly distribute the rating data of each movie to multiple clients so that the weight can be ignored when calculating the average rating.
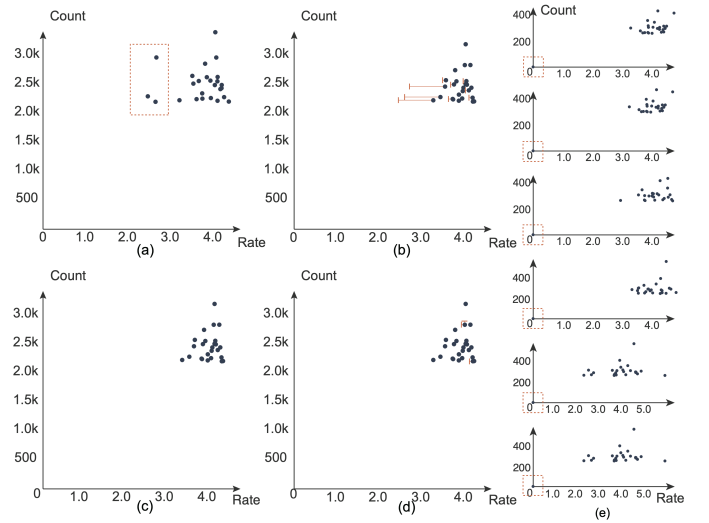

Fig. 8. The visualization result of the *query-based* scheme (a) and the *predition-based* scheme (c). The error chart of the the *query-based* scheme (b) and the *predition-based* scheme (d). There are many client views which contain dots at (0,0), as marked by the red dashed boxes in (e).

First, the user chooses the *query-based* mode and analyzes the ratings of movies of interest using a scatterplot. The scatterplot integrates the rating and the number of rating records of all clients. Each point in the scatterplot represents a movie. Under our federated visualization framework, he can see more comprehensive patterns while protecting privacy.

However, when he observes the ratings of the movies "Godfather, The " (1972), "Star Wars: Episode IV - A New Hope" (1977), "Titanic" (1997), he notices that the RE presented in the server performance panel is 0.015, which is relatively large compared with other results. Then he switches to the error chart and observes that the errors of these three movies are relatively large, as shown in Figure 8 (b). In the client view, he notices several clients have points at (0, 0), which means that the client does not have corresponding

movie rating data (Figure 8 (e)). Specifically, he finds that there is no rating data for "Star Wars: Episode IV-A New Hope" (1977) in the clients 1, 2 and 5, and there is no rating data for "Godfather, The" (1972) and "Titanic" (1997) in the clients 6, 7, and 8. With the *query-based* scheme, each client needs to upload visual feature vectors of the same length. Each item in the vector corresponds to the value of a visual feature index. If there is no data corresponding to a certain index locally, the value will be automatically filled with 0. In this case, when there is no movie rating data, that is, when there is no data corresponding to this index locally, its value is processed as 0. This causes the movie rating to be pulled down in the global visualization. In addition, for this kind of missing data situation, the *query-based* scheme is not always incorrect. If the visual feature is obtained by counting items, it makes sense to treat no data record for a certain visual feature index as 0. This means that there is no data record that meets the query conditions.

The *prediction-based* scheme can be well compatible with this situation. Figure 8 (c) shows the result of the same aggregated visual query, with relatively small errors. This is because the *prediction-based* scheme does not handle missing data items. For example, in this case, to fit the average rating of "Star Wars: Episode IV-A New Hope" (1977), only the data in the clients 3, 4, 6, 7, 8 are involved in the training to ensure the accuracy of the results. The *prediction-based* scheme requires federated model training. As the training round increases, the RE of the visualization results decreases. The training process makes the response time of the *prediction-based* scheme longer than that of the *query-based* scheme. In short, if the user's analysis scenario is complex, which requires better compatibility and does not require fast response time, the *prediction-based* scheme can be used. If the user needs a fast response time, he can choose the *query-based* scheme.

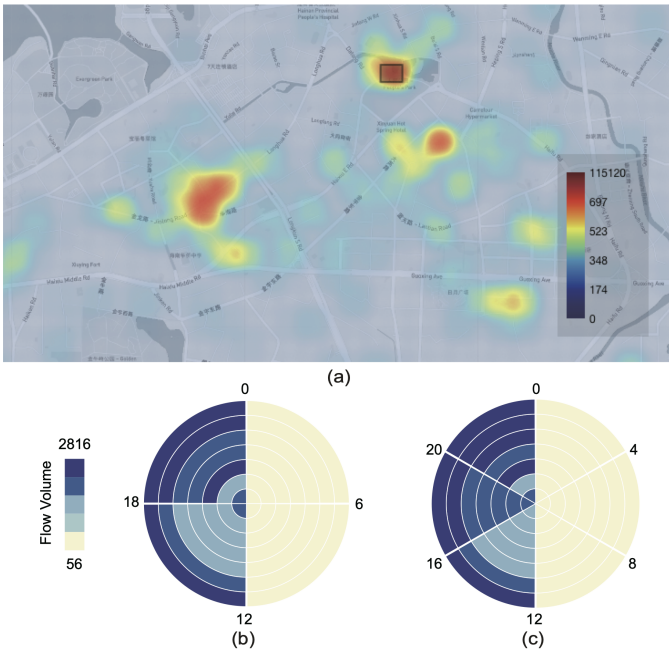### 5.2.3 Case Three: Urban data exploration

(a)

(b)   (c)

Fig. 9. Locations near the night fair have relatively heavy traffic between 6 p.m. and 12 p.m. Adjusting the hours per arc to 4 further indicates that the traffic between 8 p.m. and 12 p.m. is heavy. The color of the bars encodes different traffic flow volumes.

First, the user chooses the *prediction-based* scheme. He uses a heatmap to analyze the traffic flow from May 1st to October 31st. Figure 5 indicates several locations of high traffic intensity. To further study the constant high intensity pattern, three locations in Figure 5 are explored. Location 1 presents the highest intensity because it contains several shopping malls and apartment districts. The same reason holds for location 2. In location 3, there is one of the most famous night fairs in the city. To validate this pattern, a polar heatmap is created using the same dimensions (Figure 9). Figure 9 (b) indicates that most traffic happens between 6 p.m. and 12 p.m. every day. After modifying the granularity of data partition, a more detailed aggregation shown in Figure 9 (c) shows that traffic between 20 pm and 24 pm have a large proportion in daily traffic.
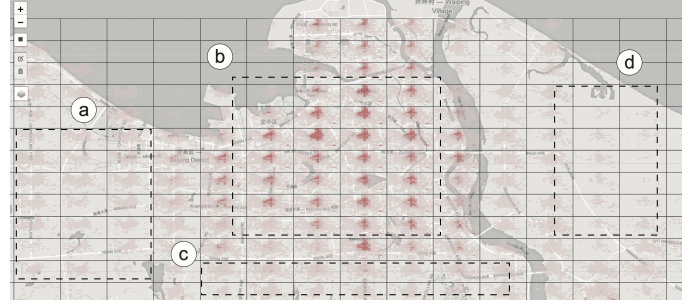

Fig. 10. Four districts with different flow patterns.

To further study the mobility modes over regions, ODMap [49] is employed to show the links among sources and destinations. It is essentially a form of origin in which rows and columns represent the locations of flow origins and the locations of destinations, respectively. Figure 10 indicates that there are different flow patterns between districts. Most grids in the center of ODMap present a similar distribution and high intensity, while grids in the left part, bottom part, and right part exhibit distinctive distributions. These lead to two observations: four different districts present four different mobility modes; the downtown region has the highest intensity in both the heatmap and ODMap.

In short, the federated visualization framework can support the privacy-preserving visualization of the aggregated visual query.

5.3 Expert Interview

To evaluate the effectiveness of federated visualization, we conducted one-on-one interviews with three experts.

Background. All experts have experience in visual analysis. In a prior discussion, they agreed that privacy is a big concern in visually analyzing decentralized data. A comprehensive analysis of a problem is not possible if data can not be shared. They have no knowledge of federated visualization.

Process. In each interview, we first introduced the background of federated visualization, our visual interface and chart examples in the gallery, and then demonstrated how the system works with the first case. Then we asked them to freely explore three datasets, answer their questions, and observe their behaviors. Finally, we collected their feedback. This process took approximately 60 minutes.

Feedback. Overall, all experts felt that our system has no difference from conventional visual analysis systems and can be easily analyzed. They confirmed this convenience with various chart types and some basic interactions. An expert liked the provision of different accuracy levels in the system, which makes it flexible for

different privacy scenarios. Surely, low accuracy has little influence on visual distributions but can shorten the system response time. An expert tried to re-identify an arbitrary individual but failed. This verifies the effectiveness of our system.

All experts commented, "*It takes a long time to refresh the heatmap and ODMap interactively, while the polar heatmap can be refreshed in real-time.*" To handle complex charts and large datasets, schemes for optimizing query performance, like the pre-computation scheme, could be incorporated in the future. An expert reported, "*I cannot feel the results are inaccurate, and I am not confident in the results of the analysis.*" And he further suggested that we present the inaccuracy of the result. For example, visual encodings of uncertainty can be strengthened to clarify the inaccuracy. They also discussed the possibility of using federated visualization to create complicated visualizations. They hoped that our approach could be extended to support complex scenarios such as graph data or multi-source datasets from different domains.

6 DISCUSSION

Below, we discuss our work in terms of generality, privacy-preserving, and performance. We also summarize the limitations and suggest directions for further work.

Generality. Case studies on several visual forms verify the effectiveness of our approach. Actually, our approach is applicable to all visualization charts that can be generated through data aggregation (mean and addition). Essentially, our approach aggregates visual features from each client without obtaining the specific raw data of each client. This means that if visual features of a chart can be obtained by summing data attributes, privacy-preserving visualization is feasible. For example, creating a pie chart needs to count the amount of data items for corresponding sectors from clients.

The *prediction-based* scheme has better generality than the *query-based* scheme. In particular, the *query-based* scheme may yield less accuracy when there are missed attribute values. For example, the server needs to use data from three clients (C_1,C_2,C_3) to visualize the probability of two events E_A and E_B. Both the data held by C_1 and C_2 can be used to calculate the probability of two events, while C_3 can only obtain the probability of E_A and does not know the probability of E_B. In this case, the *query-based* scheme with which each client needs to send all visual features does not work. If the probability of E_B is set to be zero by C_3 to complement all visual features to participate in federated visualization, the overall accuracy decreases, because the client does not know the probability of E_B. In contrast, the *prediction-based* scheme works in this scenario. If some attribute values are missing in a client, the client only employs existing data for local training. The missing data does not affect accuracy.

Privacy preservation. Secure aggregation [34] is widely used in federated learning to encrypt the model gradients of each client and avoid backtracking the original data. Secure aggregation can guarantee privacy under the threat conditions of *server is honest-but-curious* and *server can lie to client*, that is, all clients follow the protocol honestly, but the server may try to learn additional information in different ways. However, collusion among clients can result in privacy leakage. Our approach employs secure aggregation to protect the privacy of transported parameters. In our implementation, if four of the five clients collude with each other, the four clients send invalid information to the server, such as zero.

Consequently, the composed visualization only shows the data of the innocent client, which may lead to privacy exposure.

Conventional approaches seek to protect privacy through data anonymity. However, simply anonymizing data would lead to low utility. The visualization based on anonymized data might exhibit incorrect patterns and mislead the decision. Our approach aggregates data to obtain visual features and allows for secured visual analysis within the federated visualization framework. As such, global visual features are relatively accurate.

Performance. Several factors, such as response time and accuracy, may influence the performance of federated visualization. Compared with traditional centralized visualization, our approach has extra time overhead to achieve privacy protection. The *query-based* scheme integrates encrypted visual features on the server side and computes the sum of visual features of each client without loss. Data encryption transmission costs extra response time. The *prediction-based* scheme uses the data on each client to train a global model to fit global visual features. Ideally, its accuracy can reach 100%. However, in real scenarios, models are often unable to fit completely because of time constraints, data distributions (non-i.i.d. or i.i.d.), or federated learning characteristics. Quantitative results show that the time increases with the accuracy. A balance between accuracy and time can be achieved. In addition, as the amount of data required to create visual charts increases, obtaining more accurate results is more time-consuming. There is much capacity for further performance optimization. For example, the level-of-details scheme can be employed in visualizing a heatmap.

The *query-based* scheme can generate more accurate results than the *prediction-based* scheme and has better running performance. Thus, it is more feasible for time-critical situations.

Limitations and future work. First, the number of clients should be larger than 3. Otherwise, the collected information on the server can be used to infer secure information. Second, clients should make a strict protocol agreement and be honest because our approach can not identify collusion among clients. Third, our *prediction-based* scheme re-trains the model after each user interaction. When the number of visual features to be trained reaches tens of thousands, the response time becomes even longer, resulting in an unfriendly user experience. In the future, we can integrate more schemes into our federated visualization framework, not limited to aggregated visual queries.

7 CONCLUSION

This paper addresses an important aspect of decentralized visualization: privacy. The fundamental idea is to mimic the process of federated learning, and reformulate the visualization process with a new federated model. We propose two implementations: a *query-based* scheme, and a *prediction-based* scheme.

The *query-based* scheme directly encrypts accurate results, resulting in relative short response time than the *prediction-based* scheme. The *prediction-based* scheme can be inefficient when the parameter number of the prediction model is large, i.e., more than ten thousands. We plan to reduce its computational complexity. Our work is the first attempt to tackle data privacy issues in a decentralized visualization framework. We hope that this work will inspire other researchers to further study the privacy preservation solution in distributed environment, which should be a meaningful direction for sensitive data collaborative analysis.

ACKNOWLEDGMENTS

REFERENCES

[1] S. M. Plis, A. D. Sarwate, D. Wood, C. Dieringer, D. Landis, C. Reed, S. R. Panta, J. A. Turner, J. M. Shoemaker, K. W. Carter *et al.*, "COINSTAC: A Privacy Enabled Model and Prototype for Leveraging and Processing Decentralized Brain Imaging Data," *Frontiers in Neuroscience*, vol. 10, p. 365, 2016.

[2] D. K. Saha, V. D. Calhoun, S. R. Panta, and S. M. Plis, "See Without Looking: Joint Visualization of Sensitive Multi-site Datasets," in *Proceedings of the Twenty-Sixth International Joint Conference on Artificial Intelligence*, 2017, pp. 2672–2678.

[3] J. Oksanen, C. Bergman, J. Sainio, and J. Westerholm, "Methods for deriving and calibrating privacy-preserving heat maps from mobile sports tracking application data," *Journal of Transport Geography*, vol. 48, pp. 135–144, 2015.

[4] X. Wang, T. Gu, X. Luo, X. Cai, T. Lao, W. Chen, Y. Wu, J. Yu, and W. Chen, "A User Study on the Capability of Three Geo-based Features in Analyzing and Locating Trajectories," *IEEE Transactions on Intelligent Transportation Systems*, vol. 20, no. 9, pp. 3375–3385, 2018.

[5] W. Chen, Z. Huang, F. Wu, M. Zhu, H. Guan, and R. Maciejewski, "VAUD: A Visual Analysis Approach for Exploring Spatio-Temporal Urban Data," *IEEE Transactions on Visualization and Computer Graphics*, vol. 24, no. 9, pp. 2636–2648, 2017.

[6] Z. Zhou, L. Meng, C. Tang, Y. Zhao, Z. Guo, M. Hu, and W. Chen, "Visual Abstraction of Large Scale Geospatial Origin-Destination Movement Data," *IEEE Transactions on Visualization and Computer Graphics*, vol. 25, no. 1, pp. 43–53, 2018.

[7] K. W. Brodlie, D. A. Duce, J. R. Gallop, J. P. Walton, and J. D. Wood, "Distributed and Collaborative Visualization," *Computer Graphics Forum*, vol. 23, no. 2, pp. 223–251, 2004.

[8] A. Dasgupta, E. Maguire, A. Abdul-Rahman, and M. Chen, "Opportunities and Challenges for Privacy-Preserving Visualization of Electronic Health Record Data," in *Proceedings of the IEEE VIS Workshop on Visualization of Electronic Health Records*, 2014.

[9] X. Wang, J.-K. Chou, W. Chen, H. Guan, W. Chen, T. Lao, and K.-L. Ma, "A Utility-aware Visual Approach for Anonymizing Multi-attribute Tabular Data," *IEEE Transactions on Visualization and Computer Graphics*, vol. 24, no. 1, pp. 351–360, 2017.

[10] X. Wang, W. Chen, J.-K. Chou, C. Bryan, H. Guan, W. Chen, R. Pan, and K.-L. Ma, "GraphProtector: A Visual Interface for Employing and Assessing Multiple Privacy Preserving Graph Algorithms," *IEEE Transactions on Visualization and Computer Graphics*, vol. 25, no. 1, pp. 193–203, 2018.

[11] A. Dasgupta and R. Kosara, "Adaptive Privacy-Preserving Visualization Using Parallel Coordinates," *IEEE Transactions on Visualization and Computer Graphics*, vol. 17, no. 12, pp. 2241–2248, 2011.

[12] X.-M. Wang, T.-Y. Zhang, Y.-X. Ma, J. Xia, and W. Chen, "A survey of visual analytic pipelines," *Journal of Computer Science and Technology*, vol. 31, no. 4, pp. 787–804, 2016.

[13] R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu, "Hippocratic Databases," in *Proceedings of the 28th International Conference on Very Large Databases*, 2002, pp. 143–154.

[14] L. Sweeney, "*k*-anonymity: A model for protecting privacy," *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, vol. 10, no. 5, pp. 557–570, 2002.

[15] A. Machanavajjhala, D. Kifer, J. Gehrke, and M. Venkitasubramaniam, "*l*-Diversity: Privacy Beyond *k*-Anonymity," *ACM Transactions on Knowledge Discovery from Data*, vol. 1, no. 1, p. 3, 2007.

[16] N. Li, T. Li, and S. Venkatasubramanian, "*t*-Closeness: Privacy Beyond *k*-Anonymity and *l*-Diversity," in *Proceedings of the IEEE 23rd International Conference on Data Engineering*, 2007, pp. 106–115.

[17] J. Cao and P. Karras, "Publishing microdata with a robust privacy guarantee," in *Proceedings of the VLDB Endowment*, 2012, pp. 1388–1399.

[18] J. Soria-Comas and J. Domingo-Ferrert, "Differential privacy via t-closeness in data publishing," in *2013 Eleventh Annual Conference on Privacy, Security and Trust*. IEEE, 2013, pp. 27–35.

[19] J.-K. Chou, Y. Wang, and K.-L. Ma, "Privacy Preserving Event Sequence Data Visualization using a Sankey Diagram-like Representation," in *Proceedings of the SIGGRAPH ASIA Symposium on Visualization*, 2016, pp. 1–8.

[20] ——, "Privacy Preserving Visualization: A Study on Event Sequence Data," *Computer Graphics Forum*, vol. 38, no. 1, pp. 340–355, 2019.

[21] A. Dasgupta, R. Kosara, and M. Chen, "*Guess Me If You Can*: A Visual Uncertainty Model for Transparent Evaluation of Disclosure Risks in Privacy-Preserving Data Visualization," in *Proceedings of the IEEE Symposium on Visualization for Cyber Security*, 2019.

[22] W. Chen, Y. Wei, Z. Wang, S. Zhou, B. Lin, and Z. Zhou, "Federated visualization: A privacy-preserving strategy for decentralized visualization," *arXiv preprint arXiv:2007.15227*, 2020.

[23] S. Lefebvre and H. Hoppe, "Perfect Spatial Hashing," *ACM Transactions on Graphics*, vol. 25, no. 3, pp. 579–588, 2006.

[24] J. Xie, H. Yu, and K.-L. Ma, "Visualizing Large 3D Geodesic Grid Data with Massively Distributed GPUs," in *Proceedings of the IEEE 4th Symposium on Large Data Analysis and Visualization*, 2014, pp. 3–10.

[25] M. Shih, S. Rizzi, J. Insley, T. Uram, V. Vishwanath, M. Hereld, M. E. Papka, and K.-L. Ma, "Parallel Distributed, GPU-Accelerated, Advanced Lighting Calculations for Large-Scale Volume Visualization," in *Proceedings of the IEEE 6th Symposium on Large Data Analysis and Visualization*, 2016, pp. 47–55.

[26] A. Meidiana, S.-H. Hong, J. Huang, P. Eades, and K.-L. Ma, "Topology-Based Spectral Sparsification," in *Proceedings of the IEEE 9th Symposium on Large Data Analysis and Visualization*, 2019, pp. 73–82.

[27] A. Arleo, O.-H. Kwon, and K.-L. Ma, "GraphRay: Distributed Pathfinder Network Scaling," in *Proceedings of the IEEE 7th Symposium on Large Data Analysis and Visualization*, 2017, pp. 74–83.

[28] J. Konečnỳ, H. B. McMahan, F. X. Yu, P. Richtárik, A. T. Suresh, and D. Bacon, "Federated learning: Strategies for improving communication efficiency," in *NIPS Workshop on Private Multi-Party Machine Learning*, 2016.

[29] T. Li, A. K. Sahu, A. Talwalkar, and V. Smith, "Federated learning: Challenges, methods, and future directions," *IEEE Signal Processing Magazine*, vol. 37, no. 3, pp. 50–60, 2020.

[30] X. Wei, Q. Li, Y. Liu, H. Yu, T. Chen, and Q. Yang, "Multi-agent visualization for explaining federated learning." in *Proceedings of the Twenty-Eighth IJCAI*, 2019, pp. 6572–6574.

[31] J. Konečnỳ, H. B. McMahan, D. Ramage, and P. Richtárik, "Federated Optimization: Distributed Machine Learning for On-Device Intelligence," *arXiv preprint arXiv:1610.02527*, 2016.

[32] H. B. McMahan, D. Ramage, K. Talwar, and L. Zhang, "Learning Differentially Private Recurrent Language Models," in *International Conference on Learning Representations*, 2018.

[33] R. C. Geyer, T. Klein, and M. Nabi, "Differentially Private Federated Learning: A Client Level Perspective," *arXiv preprint arXiv:1712.07557*, 2017.

[34] 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," in *NIPS Workshop on Private Multi-Party Machine Learning*, 2016.

[35] L. Huang, A. L. Shea, H. Qian, A. Masurkar, H. Deng, and D. Liu, "Patient clustering improves efficiency of federated machine learning to predict mortality and hospital stay time using distributed electronic medical records," *Journal of Biomedical Informatics*, vol. 99, p. 103291, 2019.

[36] L. Huang, Y. Yin, Z. Fu, S. Zhang, H. Deng, and D. Liu, "Loadaboost: Loss-based adaboost federated machine learning with reduced computational complexity on iid and non-iid intensive care data," *Plos one*, vol. 15, no. 4, p. e0230706, 2020.

[37] M. Y. Lu, R. J. Chen, D. Kong, J. Lipkova, R. Singh, D. F. Williamson, T. Y. Chen, and F. Mahmood, "Federated learning for computational pathology on gigapixel whole slide images," *Medical image analysis*, vol. 76, p. 102298, 2022.

[38] J. Kang, D. Ye, J. Nie, J. Xiao, X. Deng, S. Wang, Z. Xiong, R. Yu, and D. Niyato, "Blockchain-based federated learning for industrial metaverses: Incentive scheme with optimal AoI," in *2022 IEEE International Conference on Blockchain (Blockchain)*, 2022, pp. 71–78.

[39] H. Moayyed, A. Moradzadeh, B. Mohammadi-Ivatloo, A. P. Aguiar, and R. Ghorbani, "A Cyber-Secure generalized supermodel for wind power forecasting based on deep federated learning and image processing," *Energy Conversion and Management*, vol. 267, p. 115852, 2022.

[40] D. Połap and M. Woźniak, "A hybridization of distributed policy and heuristic augmentation for improving federated learning approach," *Neural Networks*, vol. 146, pp. 130–140, 2022.

[41] Y. Liu, A. Huang, Y. Luo, H. Huang, Y. Liu, Y. Chen, L. Feng, T. Chen, H. Yu, and Q. Yang, "FedVision: An online visual object detection platform powered by federated learning," in *Proceedings of the AAAI Conference on Artificial Intelligence*, vol. 34, no. 08, 2020, pp. 13 172–13 179.

[42] J. Pei, K. Zhong, M. A. Jan, and J. Li, "Personalized federated learning framework for network traffic anomaly detection," *Computer Networks*, vol. 209, p. 108906, 2022.

[43] X. Wang, W. Chen, J. Xia, Z. Wen, R. Zhu, and T. Schreck, "HetVis: A Visual Analysis Approach for Identifying Data Heterogeneity in Horizontal Federated Learning," *IEEE Transactions on Visualization and Computer Graphics*, vol. 29, no. 1, pp. 310–319, 2022.

[44] Q. Yang, Y. Liu, T. Chen, and Y. Tong, "Federated Machine Learning: Concept and Applications," *ACM Transactions on Intelligent Systems and Technology*, vol. 10, no. 2, pp. 1–19, 2019.

[45] B. Ramsundar and R. B. Zadeh, *TensorFlow for Deep Learning: From Linear Regression to Reinforcement Learning*, 2018.

[46] C. Dwork, F. McSherry, K. Nissim, and A. Smith, "Calibrating noise to sensitivity in private data analysis," in *Theory of cryptography conference*. Springer, 2006, pp. 265–284.

[47] H. Mei, W. Chen, Y. Wei, Y. Hu, S. Zhou, B. Lin, Y. Zhao, and J. Xia, "RSATree: Distribution-Aware Data Representation of Large-Scale Tabular Datasets for Flexible Visual Query," *IEEE Transactions on Visualization and Computer Graphics*, vol. 26, no. 1, pp. 1161–1171, 2019.

[48] Y. Zhao, M. Li, L. Lai, N. Suda, D. Civin, and V. Chandra, "Federated Learning with Non-IID Data," *arXiv preprint arXiv:1806.00582*, 2018.

[49] J. Wood, J. Dykes, and A. Slingsby, "Visualisation of origins, destinations and flows with od maps," *The Cartographic Journal*, vol. 47, no. 2, pp. 117–129, 2010.

Shuyue Zhou received the MS degree at 2021 at Zhejiang University, China. She's now working in Alibaba, Hangzhou, China. Her research interests include information visualization and visual analytics.

Bingru Lin received the master degree at 2020 at Zhejiang University, China. He is now working in Alibaba Group, Hangzhou, China. His research interests include information visualization and visual analytics.

Wei Chen is a professor in the State Key Lab of CAD&CG, Zhejiang University. His research interests include visualization and visual analysis, and has published more than 70 IEEE/ACM Transactions and IEEE VIS papers. He actively served as guest or associate editors of the ACM Transactions on Intelligent System and Technology, the IEEE Computer Graphics and Applications and Journal of Visualization.

Yating Wei is a Ph.D. student in the State Key Lab of CAD&CG at Zhejiang University, Hangzhou. She earned the B.S. degree in software engineering from Central South University in 2017. Her research interests are visual analytics and perceptual consistency.

Zhiguang Zhou is a professor in the Hangzhou Dianzi University. His research interests include information visualization, visual analytics. Zhou has a doctor degree in computer science from Zhejiang University.

Zhiyong Wang received the MS degree at 2022 at Zhejiang University, China. He is now working in Tencent, Guangzhou, China. His research interests include federated learning and visual analytics.