IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 29 February 2024, accepted 18 March 2024, date of publication 25 March 2024, date of current version 29 March 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3380195

RESEARCH ARTICLE

DP-FedIOD: A Differential Privacy and Federated Learning Based Framework for Aerial Insulators Orientation Detection

XUEJUN ZHANG, XIAO ZHANG, XIAOWEN SUN, FENGHE ZHANG, BIN ZHANG, CHENGZE LI, AND XIAOHONG JIA

School of Electronic and Information Engineering, Lanzhou Jiaotong University, Lanzhou 730070, China

Corresponding author: Xiao Zhang (zhangxiao.617@icloud.com)

This work was supported in part by the National Natural Science Foundation of China under Grant 61762058 and Grant 62366029; in part by the Youth Science and Technology Fund Project of Gansu Province, China, under Grant 23JRRA855; in part by the Special Fund for Postdoctoral Fellowships of Gansu Province, China, under Grant 23JRRA863; in part by the Industry Support Project of Gansu Province, China, under Grant 2022CYZC-38; and in part by the Science and Technology Project of the Research Institute of Electric Power Science and Technology of State Grid Gansu Electric Power Company under Grant 522722220013.

ABSTRACT To address the limitations of deep learning models in detecting aerial insulator images from Unmanned Aerial Vehicles, we present a framework dubbed DP-FedIOD, which utilizes differential privacy and federated learning techniques for identifying the aerial insulators. It tackles the issue posed by current algorithms for inspecting insulators, which employ horizontal anchor frames and are incapable of precisely identifying both insulators and their defective parts. In addition, this study addresses the issue of insulator data being safeguarded by laws and policies that impede its wide-scale collection and dissemination among electric power companies enterprises, resulting in insufficient data volume to train deep learning models. In DP-FedIOD, we have improved the YOLOv5 algorithm by refining its head structure and loss function for directional detection of insulators and their defective parts. Additionally, an attention mechanism module has been incorporated into its backbone to enhance feature extraction capabilities. Furthermore, DP-FedIOD collaboratively trains the global model through federated learning. To prevent privacy leakage in the federated learning process, we also incorporate Laplace noise according to the differential privacy mechanism before uploading the weight information. The experimental outcomes demonstrate that the improved YOLOv5 model attains a mAP@0.5 metric of 95.00%, while DP-FedIOD achieves over 75.10% and 77.90% in precision and recall, respectively. These results indicate that DP-FedIOD has significant practical value in constructing an intelligent grid equipment detection system.

INDEX TERMS Differential privacy, federated learning, insulator, object detection, orientation identification.

I. INTRODUCTION

IInsulators are essential devices for controlling insulation in high voltage overhead transmission and distribution networks. Statistics regarding the number of insulators and detection of leaking caps have made safe operation of transmission and distribution networks increasingly important [1]. The significant inspection workload has made traditional human inspection methods insufficient, highlighting the need for intelligent insulator inspection research. The use of Unmanned Aerial Vehicles (UAVs) and computer vision technology has made image and video data acquisition for insulator inspection a viable alternative to manual methods. Zhai et al. [2] identified insulator target regions using RGB colors and spatial characteristics to apply computer vision for recognition and analysis. The morphological processing of the target region highlights the fault location. Wu et al. [3] extracted texture features of insulators using the gray level covariance matrix (GLCM) and differentiated texture targets using principal component analysis (PCA).

The associate editor coordinating the review of this manuscript and approving it for publication was Sedat Akleylek.

A. OBJECT DETECTION (OD)

Since the emergence of Deep learning(DL) [4] in 2012 and its widespread application, researchers have favored computer vision technology based on DL for its efficient performance, and it has been rapidly advancing. Presently, China's power operation units conduct inspections of small multi-rotor UAVs and fixed-wing UAVs [5]. Object detection technology based on DL in the field of computer vision is applied during these inspections. This technology effectively resolves several issues found in traditional object detection approaches, including lackluster robustness, extensive time complexity, inadequate region selection strategies, insufficient feature extraction techniques, and diverse classifiers. For precise object detection of insulators and their defect recognition algorithms, mainstream efforts focus on anchor frame based methods. These methods are categorized into two-stage and single-stage networks. Two-stage networks include Fast R-CNN [6], Faster R-CNN [7], and Mask R-CNN [8].Chen et al. [9] utilized a convolutional neural network and insulators contour features to detect insulators for saliency detections. Zhong et al. [10] enhanced defect detection by improving the anchor frame mechanism for candidate selection. Liao et al. [11] improved the classic Faster R-CNN by utilizing ResNet101 as the backbone feature extraction network and enhancing detection of overlapping insula-tors via soft-nms. Ling et al. [12] utilized Faster R-CNN to enhance the signal-to-noise ratio and combined it with U-Net for pixel classification to address the issue of locating insulator breakage sites in a low signal-to-noise environment. Tao et al. [13] achieved a higher accuracy in identifying insulators by designing a cascade structure based on Faster R-CNN and using data enhancement methods, including affine transformation and Gaussian fuzzy. Single-stage networks are primarily represented by the YOLO (You Only Look Once, YOLO) [14] series of networks, including YOLO, YOLOv2 [15], YOLOv3 [16], YOLOv4 [17], and YOLOv5. Adou et al. [18] utilized the YOLOv3 network for rapid identification of insulators and detection of defects. Liu et al. [19] deepened the spatial pyramidal pooling structure of the YOLOv4 network and introduced weight coefficients to the balanced cross entropy to increase the loss function's contribution. Hao et al. [20] incorporated an attention mechanism into the YOLOv5 network to detect faults in transmission lines while retaining the network's fast detection capability. Zhang et al. [21] improved the feature extraction network of YOLOv7 by incorporating the CBAM attention mechanism and a centralized pyramid structure in the deeper layers. These modifications enhance the fusion of feature maps and the exchange of information, resulting in more accurate insulator detection. Huang et al. [22] optimised the dataset by performing super-resolution reconstruction of the raw power insulator inspection data using USRNet. They then improved the accuracy of insulator detection in complex backgrounds by constructing a larger detection head through changes to the multi-scale feature fusion structure of the YOLOv5 model.Wang et al. [23] improved the detection efficiency of the YOLOv5 model by lightening the residual module and adding depth separable convolution and 1×1 convolution. They also introduced the DC-SPP module in the feature extraction stage to increase the receptive field without losing detail information. This approach provides an excellent solution for the insulator detection task.Although the DL based algorithms for insulator and defect detection have illustrated impressive performance, there are still practical issues. The previous study mainly used horizontal anchor boxes for detecting insulators, disregarding the fact that insulators in aerial photographs are frequently inclined. When manually annotating insulators with horizontal bounding boxes, a substantial amount of extraneous information is included, hindering model convergence during training and resulting in imprecise localization of insulator positions during inference.

B. FEDERATED LEARNING (FL)

Moreover, existing DL based isolator and defect detection algorithms are all part of fully supervised learning, which relies on a significant amount of training data to improve model performance. As a result, they may not be appropriate in scenarios where data is limited. Nevertheless, according to the regulations set forth in the Data Security Act and the Measures for the Administration of Cyber Security in the Electric Power Industry, power operation units have a well defined range of inspection. The collected raw data on insulators often cannot be shared, as some national defense and military units collect data classified as national secrets. The inability to share data results in local silos. With only small amounts of data available, it becomes difficult to train a DL model that is both accurate and reliable. FL [24], a new paradigm of DL featuring distributed training characteristics, solves the data island problem effectively. Several nodes with data can train a global model collaboratively without sharing their data using FL. Scholars have applied this concept to computer vision tasks, such as Liu et al. [25] who implemented a federated learning version of YOLOv3 object detection model and obtained the dataset through crowd sourcing. He [26] conducted multiple computer vision tasks, such as image classification, object detection, and image segmentation, using the FL framework FEDML [27].

C. DIFFERENTIAL PRIVACY (DP)

FL has its benefits, but it also comes with concerns such as privacy leakage during model information transfer and aggregation. To address these issues, researchers are exploring methods like K-anonymization [28], homomorphic encryption [29], and DP [30]. However, the K-anonymity approach risks privacy leakage caused by the homogeneity of individual information within the subgroups. Likewise, the homomorphic encryption approach increases computational overhead to a large extent, which makes it difficult for end nodes with insufficient arithmetic power to participate in the

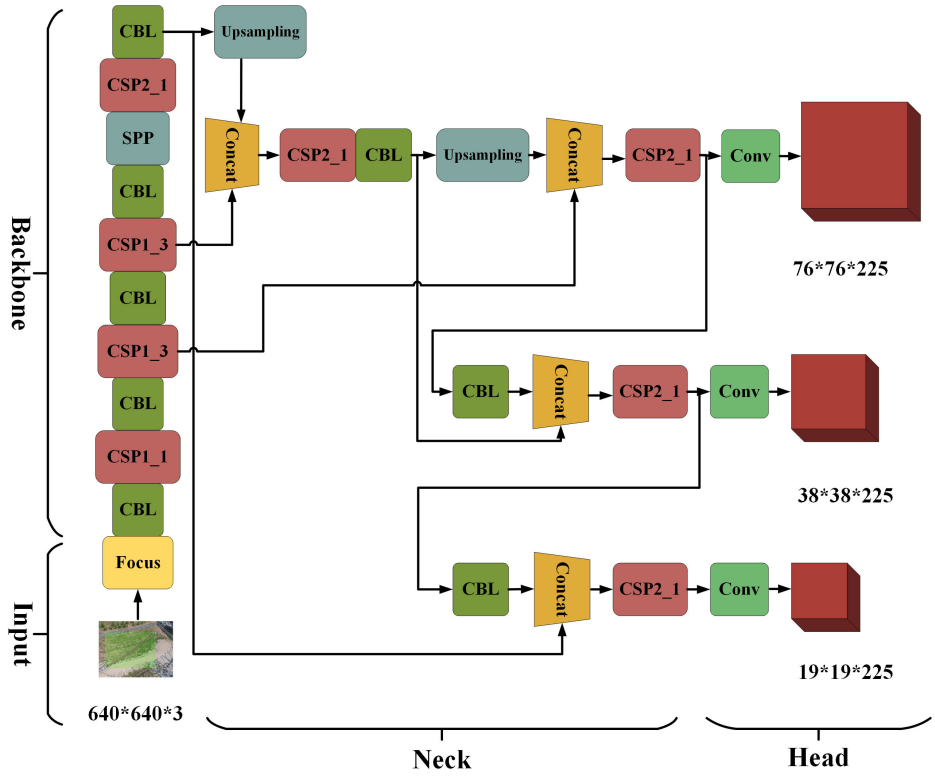

FIGURE 1. YOLOv5 model structure.

global model training. Therefore, the DP based approach for privacy preservation is widely accepted by leading researchers. For instance, Zhang et al. [31] implemented the DP technique on both the gray scale input image data and the weight parameters of the local sub-model of the deep learning indoor localization model to safeguard the user's location information. Golatkar et al. [32] applied the DP technique to enhance the visual classification problem and mitigate the effects of DP on the model by using an adaptive DP mechanism which yielded better classification accuracy.

D. CONTRIBUTIONS

The purpose of this paper is to investigate a model for detecting insulator orientation based on FL and DP. To the best of our knowledge, this is the first research to incorporate FL and DP into the task of insulator detection. The primary advancements are outlined as follows:

1) Revised YOLOv5's head structure and loss function to detect insulators and leaky cap defects directionally. Additionally, enhance the algorithm's feature extraction capability by adding a lightweight attention mechanism module to its backbone network.
2) We propose a FL based framework for detecting insulators, dubbed DP-FedIOD. The framework uses our enhanced Yolov5 algorithm for local training and weights are aggregated through weighted averaging on a cloud server. We apply Laplace noise, which satisfies ε-differential privacy, to the weight parameters prior to DP-FedIOD uploading the weight information. This approach avoids privacy leakage during the uploading process. DP-FedIOD not only addresses the issue of data silos arising from unshared data and uneven distribution, but also provides high security.
3) Experiments were carried out to verify the proposed method in this study. The outcomes suggest that the enhanced YOLOv5 mAP@0.5 attained a success rate of 95.00%. Irrespective of privacy concerns, its precision and recall both achieved rates of 80.30% and 80.90%, respectively, utilizing a distributed FL approach. In comparison, the DP-FedIOD's precision and recall exceeded rates of 75.10% and 77.90%, respectively. Therefore, these experimental results indicate that the proposed approach is both reliable and scalable.

The remainder of the paper is organized as follows. Section II provides a detailed description of the techniques used and the improvements made to them. The dataset used is presented in Section III. Section IV outlines the experiments designed to corroborate our proposed method. Finally, in Section 5, we discuss the proposed method and other relevant issues.

II. METHOD

We have upgraded the YOLOv5 network for real time object detection to have the ability to detect insulators directionally. We propose a collaborative training technique utilizing FL

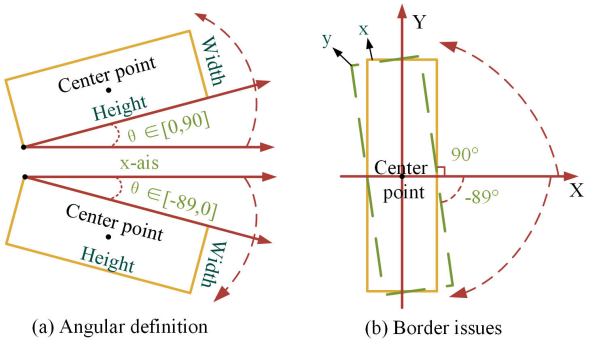

FIGURE 2. Angle definition and boundary oscillation.

to train the global model. Additionally, we incorporate the DP mechanism for preserving privacy during the weight information uploading phase of local sub-models in FL.

A. IMPROVING YOLOV5

YOLOv5 is a peer reviewed, real time object detection network in DL that has displayed outstanding performance in computer vision tasks including traffic flow detection and small target recognition since its introduction. The architecture of the YOLOv5 network is comprised of four primary components: an input module, a feature extraction module, a feature fusion module, and a prediction head, which can be viewed in Figure 1. To achieve the aim of recognizing the direction of aerial insulators and detecting their defects, our team improved the YOLOv5 network. This adaptation was founded on the directional identification study conducted by our group [33].

Most of the insulators in aerial photography appear tilted, making it difficult for the horizontal anchor frame to fit their shape accurately. To account for this, we propose using a directional anchor frame to anchor the insulators and ensure accurate framing of tilted insulators. We will redefine the label of the real frame using the long edge definition method. As shown in Figure 2 (a), the acute angle between the longer side of the rectangular frame and the horizontal direction is defined as the real frame angle θ. It is specified that the angle between the real frame and the horizontal direction is positive when above the $X-axis$ in the two-dimensional plane, and negative vice versa. The angle values θ in the range of $\theta \in [-89°, 90°]$, with 1 degree as the defined angle unit. This means that the defined angle information consists of integers. After incorporating the angle information, the data label dimension was modified from $[class, X_{topleft}, Y_{topleft}, X_{bottomright}, Y_{bottomright}]$ to $[class, X_{center}, Y_{center}, height, width, \theta]$. The YOLOv5 loss function was improved after the label information was redefined. In the original loss function of $L_{total} = L_{cls\_loss} + L_{box\_loss} + L_{con\_loss}$ being replaced by the improved loss function of $L_{total} = L_{cls\_loss} + L_{box\_loss} + L_{con\_loss} + L_{angle}$. The addition of the angle loss component to the loss function

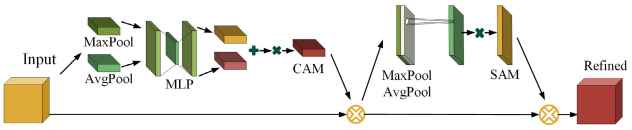

FIGURE 3. CBAM structure.

necessitated devising a sensible approach to determine the angle loss component. We have carefully considered possible solutions to this issue. If the angular loss component is treated as a regression problem, it results in the boundary oscillation issue. In Figure 2 (b), there are solid rectangular box x, dashed rectangular box y, and the horizontal direction, which form the angles 90° and −89°. If the regression problem is solved, the angular difference between the two rectangular boxes is 179 angular units. In the actual scenario, rotating 1° clockwise will make the y-box align with the x-box. In this instance, attempting to execute the regression task using the angular loss would pose challenges in achieving loss function convergence. Therefore, We opted to tackle the classification problem instead, utilizing angular losses [34]. Specifically, we constructed 180 angular classifications, where each classification denotes a feasible scenario for fitting the insulator at varying angles. This transforms the regression issue into a classification problem, naturally bypassing the problem of oscillating angular boundaries when performing the regression task. As with the original Yolov5 classification loss and the confidence loss, we compute the angular loss by means of the BCEWithlogitsloss function.

The Convolutional Block Attention Module (CBAM) [35] integrates spatial and channel information during feature extraction by convolutional neural networks. Incorporating the CBAM module into the original YOLOv5 feature extraction module can significantly enhance the capability of YOLOv5 feature extraction. Figure 3 displays its structure. CBAM primarily employs two types of pooling structures, namely global maximum pooling and global average pooling, to extract both the output channel features and spatial features. The calculation of the channel attention mechanism is denoted as Equation 1.

$$\begin{aligned} M_c(F) &= \sigma\left(MLP\left(MaxPool(F)\right) + MLP\left(AvgPool(F)\right)\right) \\ &= \sigma\left(W_1\left(W_0\left(F^c_{Max}\right)\right) + W_1\left(W_0\left(F^c_{Avg}\right)\right)\right) \end{aligned} \quad (1)$$

where the channel attention mechanism (M_c), feature (F), sigmoid activation function (σ), Multilayer Perceptron (MLP) with two layers of weights ($W_1$and W_0), and global maximum pooling (F^c_{Max}) and global average pooling (F^c_{Avg}) results comprise the channel attention mechanism.To improve the nonlinearity, it is necessary to demonstrate that the ReLU operation is established between W_0 and W_1 in the MLP of CAM. The MLP in CAM also utilises dimensionality reduction in its first layer to decrease parameter computation. The formula for the spatial attention mechanism is denoted as

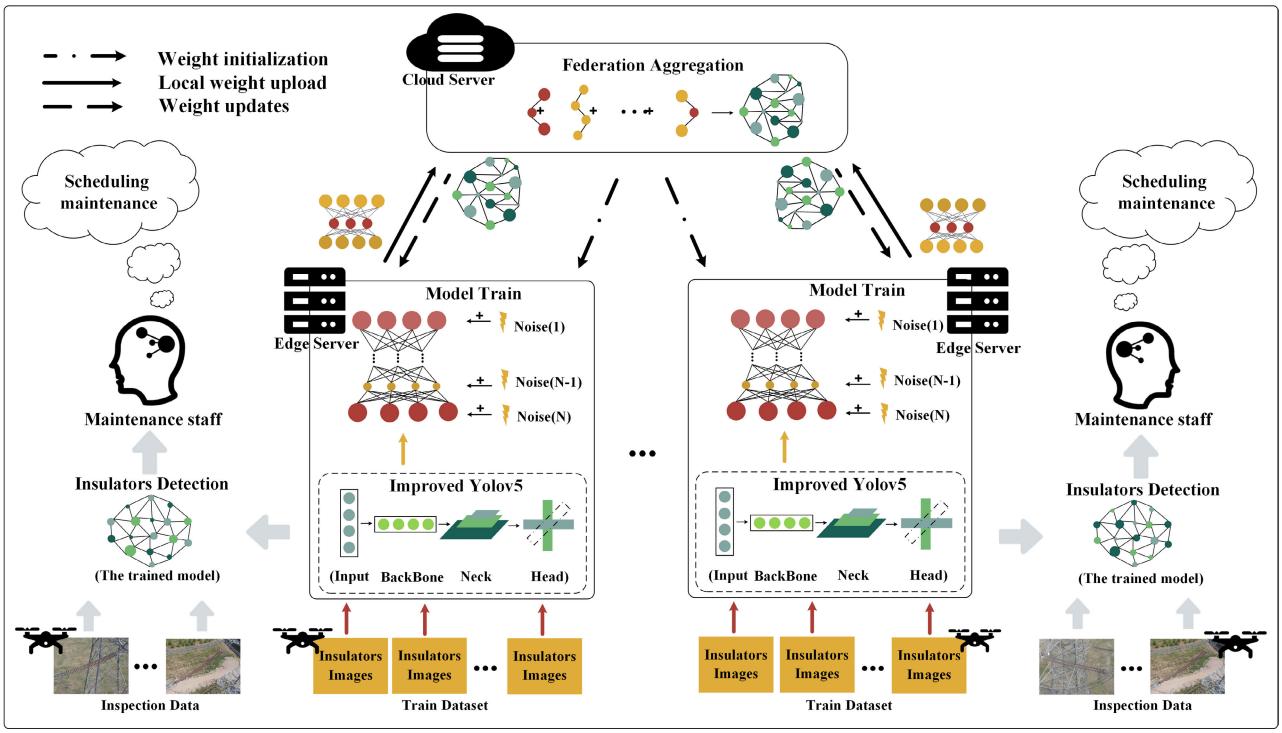

FIGURE 4. DP-FedIOD workflow schematic.

Equation 2.

$$M_s(F) = \sigma\left(f^{7*7}\left([MaxPool(F); AvgPool(F)]\right)\right) = \sigma\left(f^{7*7}\left(F^s_{Max}; F^s_{Avg}\right)\right) \quad (2)$$

$M_s$represents the spatial attention mechanism, f^{7*7}indicates the convolution operation using a convolution kernel size of 7*7, while F^s_{Max} and F^s_{Avg} denote the global maximum pooling and global average pooling outcomes in the spatial attention mechanism, correspondingly.

B. FEDERATED LEARNING

FL is a distributed approach to training that utilizes datasets distributed across participants and fuses data information from multiple parties, through various aggregation techniques to collaboratively build global models.

Based on the overlap between the feature space and sample ID space of various data owners, there are three categories of FL: horizontal federation learning(HFL) [36], vertical federation learning(VFL), and federation migration learning. HFL is suitable when the data features of the federated learning participants overlap, indicating that the data features are the same among the participants, but the data samples owned by the participants are different. When constructing a co-training task and defect detection model for insulators, if power operation units A and B cannot share data due to policy or legal reasons. And they may collect insulator images from different environments with similar characteristics. A and B can then co-develop a DL model using HFL to enhance the model's ability to generalize.

To address the challenge of sharing and distributing insulators' raw data, which renders traditional centralized training unfeasible, we introduce a FL and DP based training framework named DP-FedIOD for distributed insulator identification and its fault detection model. As depicted in Figure 4, DP-FedIOD contains three tiers: (1) data collection equipments for insulators, (2) local edge servers and (3) the cloud server. The training framework workflow is as follows: Each power operation unit utilizes UAVs to capture images of insulators within their respective jurisdictions. Subsequently, the gathered data is uploaded to the local edge servers. We do not offer privacy protection for this process due to its contextual nature. There are various ways in which the data is aggregated to the edge servers, including manual copying from the drone's storage device or network delivery. The edge servers preprocess the raw data and label it as datasets, which serve as input for the models deployed on the edge servers. During the training initiation stage, the cloud server transmits the initialization weight parameters to the edge servers. The edge servers locally train models employing the pre-weights obtained from prior training. Upon completing one iteration cycle of training, the weight data gathered during this round is uploaded to the cloud server for weights aggregation. Before this weight information is uploaded, it is perturbed by Laplace noise, which is meeting the DP mechanism criteria outlined in Section *DIFFERENTIAL PRIVACY*. Then, once the aggregation process is complete, the weight information is

Algorithm 1 The Algorithm of Federated Averaging

Require: The K clients are indexed by k; B is the local minibatch size, E is the number of local epochs, and η is the learning rate.

CloudServer executes:

Initialize w_0
for each round to $t = 1, 2, \ldots, n$ **do**
  $m \leftarrow max(C \cdot K, 1)$
  $S_t \leftarrow$ random set of m edgeServerclients
  for each client to $k \in S_t$ **do**
    $w^k_{(t+1)} \leftarrow EdgeServerClientUpdate(k, w_t)$
    $m_t \leftarrow \Sigma_{k \in S_t} n_k$
    $w_{t+1} \leftarrow \sum_{k \in S_t} \frac{n_k}{m_t} w^k_{t+1}$
  end for
end for

EdgeServerUpdate(k,w): //Run in Edge Servers

$B \leftarrow$ split P_k into batches of size B
for each local epoch I, *from* 1 *to* E **do**
  for batch to $b \in B$ **do**
    $w \leftarrow w - \eta \nabla l(w; b)$
  end for
end for
$w' \leftarrow AddLpalaceNoise(w)$
return $w'$to Cloudserver

transmitted from the cloud to the edge servers to serve as the starting weights for the next iteration. This process is then repeated for the designated number of epochs. Specifically, we use Fedavg algorithm as the cloud server parameter aggregation algorithm, Fedavg algorithm takes weighted average of the uploaded parameters. Algorithm 1 presents the details. One of the main reasons for using FedAvg is its suitability for power operation units that can autonomously collect insulator data and meet the training arithmetic requirements. Therefore, it is reasonable to assume that participating users have sufficient resources to collaboratively train the global model, which circumvents problems such as communication interruption and insufficient arithmetic that often need to be considered in FL. Our initial aim was to enable adequate aggregation of sub-models, therefore we have chosen to use FedAvg as the aggregation algorithm.

Compared to deploying sub-models on end user devices (UAVs) for training, DP-FedIOD opts to deploy model training on edge servers. This decision is mainly due to the fact that the insulator equipment inspection task does not necessitate strong personalization requirements. For instance, an online shopping platform's recommendation task must suggest appropriate products based on a user's individual browsing details. The browsing data of individual users possesses notable personalized features, necessitating the deployment of the model at the terminal node for up-to-date sub-model updates. Regarding the inspection of insulators, images of the insulators collected by different power companies or different data aggregation nodes have the same characteristics of insulators and their defects. There is no need to deploy the training section of the model to terminal devices, which could increase the risk of data transmission pressure and privacy breaches.

The cloud server and edge servers collaborate to execute the algorithm. Initially, the cloud server initializes pre-training weights to the edge servers. In the specified training rounds, a collection of m edge servers form the federally trained devices. The edge server involved in the training performs local parallel training and transmits the weight information obtained from the training to the cloud server after introducing Laplace noise through the Laplace noise addition algorithm. The cloud server computes the weighted average of the received weight information, The weights are determined by the ratio of the total number of samples on edge server n_k to the total number of samples across all servers m_k. Additionally, the edge server updates the weights locally through the stochastic gradient descent algorithm.

C. DIFFERENTIAL PRIVACY

The proposal for DP emerged as a solution to the challenge of privacy breaches in data-bases. This concept is accurately defined at the mathematical level and has an extensive scope of implementations, including statistics, data mining, machine learning, and the Internet of Things(IoT). It is in fact, the most prevalent technique for privacy preservation. Our FL framework incorporates the mechanism of DP to ensure confidentiality of the model weight. This section presents the relevant definitions of DP.

Definition 1: ε-Differential Privacy. Let there be a randomized algorithm M, where $\Re$ represents the set of all possible outputs. Additionally, let D and D' be two arbitrary sets of adjacent data, and $|D \oplus D'| = |(D \cup D') - (D \cap D')| = 1$.Where $S \subset \Re$, M is said to provide ε-differential privacy protection if M satisfies $\Pr[M(D) \in S] \leq e^{\varepsilon \times |D \oplus D'|} \times \Pr[M(D') \in S]$. Where $\oplus$ represents the symmetric differences between the two sets, ε denotes the privacy budget, and $\Pr[\cdot]$ stands for the probability that M produces a result on datasets D and D'. This definition ensures that the presence or absence of a single record has a minor impact on the output of the algorithm M.

Definition 2: Privacy sensitivity. With a function $Q : D \rightarrow \mathbb{R}^d$, the privacy sensitivity Δf of Q can be defined as $\Delta f = \max_{D,D'} ||Q(D) - Q(D')||_1$, where D, D' are two neighboring datasets. And $||Q(D) - Q(D')||_1$ is the L_1-Norm between $Q(D)$ and $Q(D')$. Privacy sensitivity is utilized to define the largest alteration instigated by erasing a record from the dataset, and serves as a critical factor in determining the quantity of additional noise.

Definition 3: Laplace mechanism. For a query function $f : D \rightarrow \mathbb{R}^d$ with a sensitivity of Δf, ε-differential privacy can be achieved by $f'(D) = f(D) + g_{Laplace}(\Delta f/\varepsilon).g_{Laplace}(\Delta f/\varepsilon)$represents a random noise following a Laplace distribution, and $b = \Delta f/\varepsilon$ is the scale

Algorithm 2 The Algorithm of Add Laplace Noise

Require: The w is the local model weight information to be uploaded to the cloud server; *layer* is the each tensor in the w; ε is the Privacy budget.

Add Laplace noise(w , ε)**:**

1: **for** each *layer* of w **do**
2: $sensitive \leftarrow max(layer) - min(layer)$ //Find the L_1-Norm of the layer
3: $noise \leftarrow Laplace_{noise}(sensitive, \varepsilon)$ //generate Laplace noise
4: $layer' \leftarrow layer + noise$
5: **end for**
6: **return** w'//w' is w that has been perturbed by Laplace noise

parameter. The Laplace distribution has a probability density function of $P[z, b] = \frac{1}{2b} \times e^{-\frac{|z|}{b}}, \forall z \in \mathbb{R}^d$. When applied in research, the ε value is often adjusted by researchers to regulate the level of privacy protection. As the ε value decreases and the noise level increases, the privacy protection strength increases, and conversely, when the ε value increases and noise level decreases, the privacy protection strength declines.

Definition 4: Post-processing property. Assuming that the randomized algorithm M satisfies ε-differential privacy, $F(M)$ algorithm also satisfies ε-differential privacy.

In DP-FedIOD, we add Laplace noise to the model weights that will be uploaded to the cloud server, satisfying ε-differential privacy requirements. Please refer to Algorithm 2 for the noise addition algorithm. First, the algorithm calculates the L_1-Norm for the first layer (tensor) in the weight information as the privacy sensitivity of this layer. Next, it computes the amount of noise utilizing the $Laplace_{noise}$ function in conjunction with the set ε value. Then, the algorithm proceeds to add the suitable Laplace noise to each element of that layer. The algorithm repeats this operation to add the appropriate Laplace noise to each layer of weight information. Finally, the output is the weight information perturbed by noise in a way that aligns with DP principles.

The proposed method in this paper perturbs local submodel weights on each edge server in the DP-FedIOD architecture, using Laplace noise that satisfies ε-differential privacy prior to uploading. This guarantees privacy during information transmission between edge servers and cloud servers. We analyze the security of the said method using the parallel combinatorial and serial combinations properties of DP.

Let the algorithm's privacy budget be ε, and let D_s be a local sub-model on the edge server. $M_s : D_s \rightarrow \Re$ is a randomized algorithm on D_s. Following Definition 1, we have $\forall r_s \in \Re, \Pr[M_s(D_s) = r_s] \leq e^{\varepsilon \times |D_s \oplus D'_s|} \times \Pr[M_s(D'_s) = r_s]$. Therefore, the weight upload phase of each edge server in DP-FedIOD adheres to ε-differential privacy. For DP-FedIOD as a whole, $\forall i \in \{1, 2, \cdots, N\}$, N represents the total number of participants participating in the weight upload phase of DP-FedIOD. Let the randomized algorithm $M_{s_i} : D_i \rightarrow \Re$used by participant P_i on dataset D_i meet the ε_i-differential privacy requirements, and ensure that the random processes of any two randomized algorithms M_{s_i} are independent of each other. Then, based on Definition 1, $\Pr[M_{s_i}(D_i) = r_i] \leq e^{\varepsilon_i} \times \Pr[M_{s_i}(D'_i) = r_i], \forall r_i \in \Re$ exists. Let the algorithm $M_s : \prod_{i=1}^{N} D_i \rightarrow \Re$ achieve ε-differential privacy, followed by $M_s = \{M_{s_1}, M_{s_2}, \cdots, M_{s_N}\}$. The output of randomized algorithm M_s is referred to as $O = \{r_1, r_2, \cdots, r_N\}$. As the random processes of two algorithms M_{s_i} are independent of each other, $\forall O \subset \Re, \Pr[M_s(D) = O] = \prod_{i=1}^{N} \Pr[M_{s_i}(D_i) = r_i]$ follows. It is a known fact from $|R \oplus S| \in \mathbb{N}$ that within all of $|D_i \oplus D'_i|, i \in \{1, 2, \cdots, N\}$, only one $|D_i \oplus D'_i| = 1$ exists, while the remaining neighboring datasets are classified as $|D_j \oplus D'_i| = 0, j \neq i$. So $\forall O \subset \Re$ such that

$$\begin{aligned}
\Pr[M_s(D) = O] &= \prod_{i=1}^{N} \Pr[M_{s_i}(D_i) = r_i] \\
&\leq \prod_{i=1}^{N} e^{\varepsilon_i \times |D_i \oplus D'_i|} \times \Pr[M_{s_i}(D'_i) = r_i] \\
&\leq e^{\varepsilon_i \times |D_i \oplus D'_i|} \times \sum_{i=1}^{N} \Pr[M_{s_i}(D'_i) = r_i] \\
&\leq e^{\varepsilon_i} \times \Pr[M_s(D') = O],
\end{aligned}$$

and only when $\varepsilon \geq \varepsilon_i$, there is $\Pr[M_s(D) = O] = e^{\varepsilon} \times \Pr[M_s(D') = O]$, $\varepsilon = \min\{\varepsilon | \varepsilon \geq \varepsilon_i, 1 \leq i \leq N\} = \min\{\varepsilon | \varepsilon \geq \max_{1 \leq i \leq N} \varepsilon_i\} = \max_{1 \leq i \leq N} \varepsilon_i$. This results in the randomized mechanism algorithm M_s meeting the requirements of $(\max_{1 \leq i \leq N} \varepsilon_i)$-differential privacy.

Since iterative training is necessary for the local sub-models on each edge server in DP-FedIOD, the trained sub-models are uploaded to cloud servers for aggregation. Laplace noise is added to the upload of trained weights each time. The serial combination properties of DP guide the entire process. Let ε denote the privacy budget assigned to a single edge server that falls under category $\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_i$. Here, i represents the number of uploads made. On a randomized algorithm $M : D_S \rightarrow \Re$, there exists $M = \{M_1, M_2, \cdots, M_i\}$. Keeping in mind that the output of Algorithm M is $O = \{r_1, r_2, \cdots, r_i\}$. Since the randomization processes of Algorithm $M_1, M_2, \cdots, M_i$ are independent of each other. Therefore, for $\forall O \subset \Re$, there is

$$\begin{aligned}
&\Pr[M(D_s) = O] \\
&= \Pr[M_1(D_s) = r_1] \Pr[M_2(D_s) = r_2] \\
&\quad \times \cdots \times \Pr[M_i(D_s) = r_i] \\
&\leq e^{\varepsilon_1 \times |D_s \oplus D'_s|} \times \Pr[M_1(D'_s) = r_1] \\
&\quad \times e^{\varepsilon_2 \times |D_s \oplus D'_s|} \times \Pr[M_2(D'_s) = r_2]
\end{aligned}$$

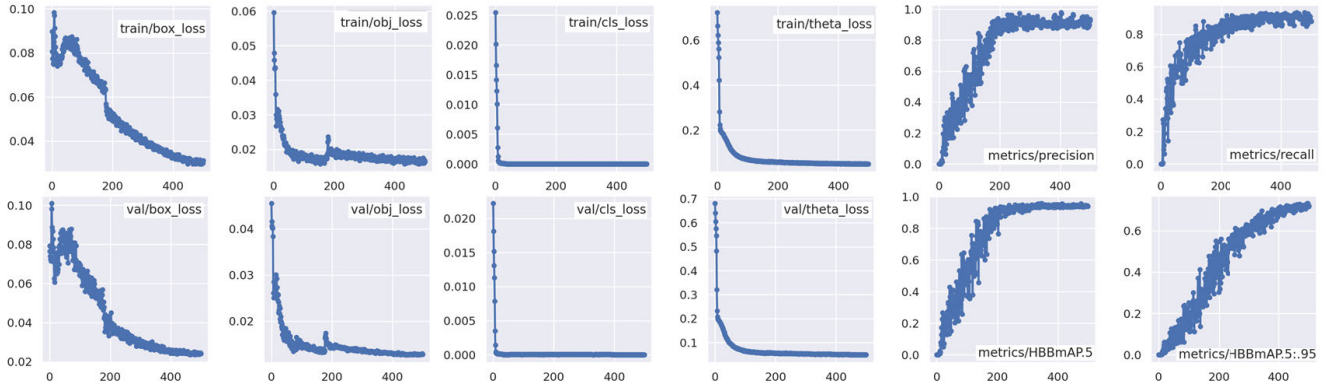

FIGURE 5. The training process for the improved YOLOv5 model.

$$\times \cdots \times e^{\varepsilon_i \times |D_s \oplus D'_s|} \times \Pr[M_i(D'_s) = r_i]$$
$$\leq e^{(\varepsilon_1+\varepsilon_2+\cdots+\varepsilon_i)\times|D_s\oplus D'_s|} \times \Pr[M(D'_s) = O].$$

From $|D_s \oplus D'_s| = 1$, we obtain $\Pr[M(D_s = O) = e^{\varepsilon_1+\varepsilon_2+\cdots+\varepsilon_i} \times \Pr[M(D'_s) = O] = e^{\varepsilon} \times \Pr[M(D'_s) = O]$. This shows that every edge server in DP-FedIOD achieves ε-differential privacy when uploading parameters.

Per Definition 4, the data disturbed by DP noise will continue to satisfy the DP mechanism post computation. Thus, there is no need to perform further differential perturbation for the aggregation model during the weight update phase of DP-FedIOD. The presented evidence indicates that DP-FedIOD meets the criteria for ε-differential privacy in the transfer of model weight information. Consequently, an attacker would be unable to conduct differential attacks through observing result output discrepancies or carry out model inversion attacks to obtain training samples or jeopardize data privacy.

III. DATASET AND EXPERIMENT

A. DATASET

We train our model using the China Power Line Insulator Dataset (CPLID [13]), which is a frequently used image set for insulator identification and defect detection tasks. We perform directional annotation of insulators and their defects using the roLableImg annotation tool to create the insulator and defect directional identification dataset. We then divide this dataset into three parts, consisting of CPLID(Train), CPLID(Test) and CPLID(Val), using a ratio of 7:2:1. The diagram in Figure 6 depicts directional annotation and traditional horizontal annotation. It is evident that the oriented frame is more suitable for fitting the insulator's profile.

B. EXPERIMENT ENVIRONMENT

Our experiments were conducted on a host with three GeForce RTX 3060 GPUs, operating on Ubuntu 20.04 LTS with an 11th Gen Intel Core i9-11900K CPU @ 3.50 GHz. The experiment consists of three phases: 1. Validating the enhanced YOLOv5 model in centralized training mode; 2. Training the global model utilizing FL; and 3. Verifying DP-FedIOD's Performance.

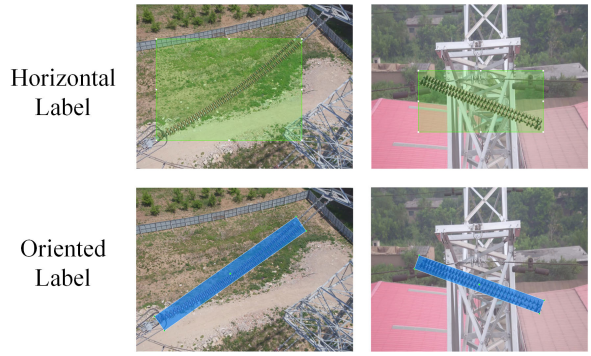

FIGURE 6. Comparison of data labels.

Precision and recall are the fundamental evaluation metrics for DL models. Other commonly used metrics, including F_1, AP, and mAP, can be calculated based on precision and recall. Therefore, this study evaluates the model using precision, recall, and $mAP@0.5$, where $mAP@0.5$ is the mAP value at the intersection and union ratio of 0.5. These metrics are computed as follows:

$$precision = \frac{TP}{TP + FP}$$
$$recall = \frac{TP}{TP + FN}$$
$$F1 = 2 \cdot \frac{precision \cdot recall}{precision + recall}$$
$$mAP = \frac{\sum_{i=1}^{N} AP_i}{N}$$

TP represents true cases, FP represents false positive cases, and FN represents false negative cases. The AP indicator can be calculated by determining the area under the PR curve. N pertains to the number of detection categories and in this paper's case, tackles the issue of monocular recognition

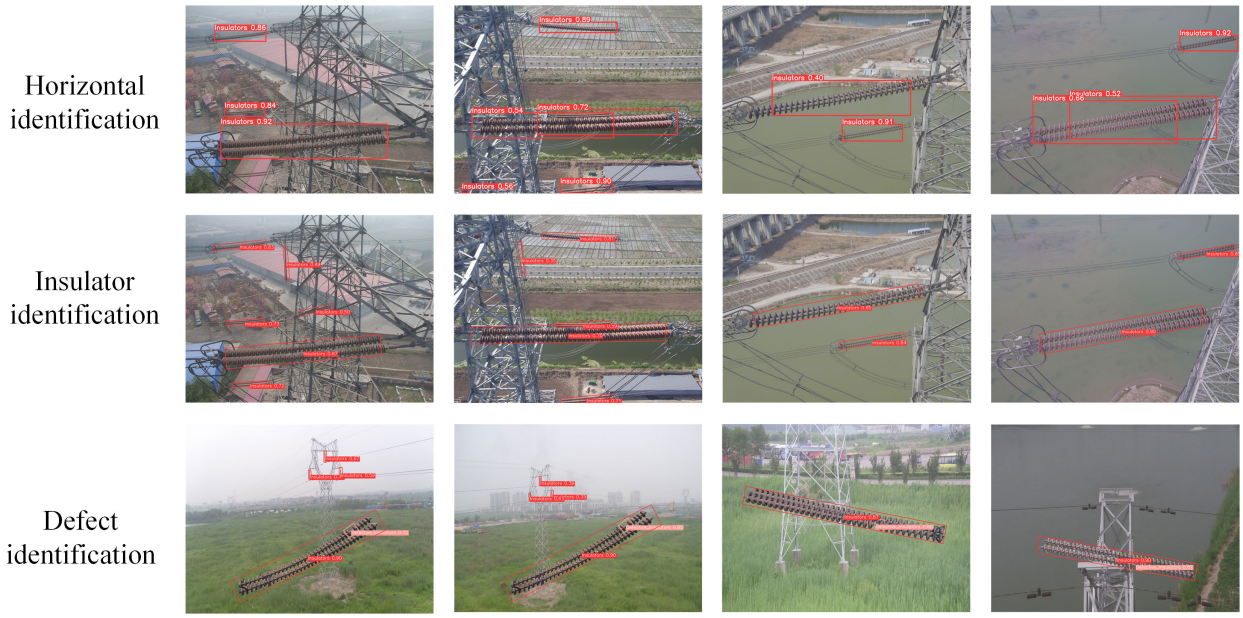

FIGURE 7. Detection effect of the improved YOLOv5 model.

($N = 1$). As such, the *mAP* indicator equals the *AP* indicator, obtainable by calculating the area under the *PR* curve.

C. IMPROVED YOLOV5 MODEL UNDER CENTRALIZED

We implemented our algorithm using pytorch 1.12.0 and utilized stochastic gradient descent (*SGD*) as the optimizer. We set the initial learning rate to 0.001, the batch size to 4, the weight decay coefficient to 0.0005, the learning rate momentum to 0.8, and ran 500 iterations.Here, we need to provide an initial explanation of the model validation details for the training process. When introducing the dataset, we divided it into three sets: CPLID(Train), CPLID(Val) and CPLID(Test), in a 7:2:1 ratio. During the actual training process, to prevent model overfitting and ensure the credibility of the validation results, not all of the CPLID(Train) was used for training.

Our model training process involves utilizing the concept of k-fold cross-validation. During each epoch, 70% of the CPLID(Train) data is randomly selected for training, while the remaining 30% is used for validation. This approach aligns with the principles of k-fold cross-validation, where the value of k represents the number of training epochs. After training the model, we conduct a final performance test using CPLID(Val) and CPLID(Test). The training process is depicted in Figure 5. In Figure 5, the loss function curves of both the training and validation phases synchronize, indicating the absence of overfitting during training. Additionally, the mAP@0.5 metric reaches 95.00%. The trained model effectively predicts the validation input, as depicted in Figure 7. Obviously, compared to the unmodified horizontal prediction frame, the oriented prediction frame can better conform to the shape of insulators, preventing unnecessary background information in frame selection and accurately locating the insulators and their defects.

TABLE 1. Model performance comparison.

Method	mAP@0.5/%	Recall/%	F1/%	Times/s
Faster R-cnn(Resnet50)	94.28	92.66	84.00	0.370
Faster R-cnn(Vgg19)	96.83	97.25	70.20	0.330
YOLOv7	94.79	93.51	94.15	0.039
YOLOv5	91.40	91.12	91.26	0.044
YOLOv5+SE	91.95	90.78	91.36	0.044
YOLOv5+ECA	92.06	91.17	91.61	0.046
YOLOv5+CBAM	92.67	92.23	92.45	0.045
YOLOv5+Orientation	93.20	90.06	91.60	0.047
ours	95.00	92.30	93.63	0.049

We compared our proposed method to several mainstream object detection algorithms, including Faster R-CNN (ResNet50 as the backbone network), Faster R-CNN (VGG19 as the backbone network), YOLOv5,and YOLOv7, on the CPLID dataset. The results of the comparison are presented in Table 1. Performance comparison, which indicates that the two-stage algorithm, represented by Faster R-CNN, performs better in terms of *mAP*@0.5 metric, but incurs a higher time overhead. The algorithm's single detection time is almost seven times higher than that of the YOLOv5 series. Our algorithm retains YOLOv5's fast detection ability and does not differ significantly from the two-stage algorithm in the *mAP*@0.5 metric.Our method outperforms YOLOv7, the current state-of-the-art model for target detection, in the mAP@0.5 metric. Although YOLOv7 is faster due to the integration of advanced training tricks. Experiments were conducted using YOLOv5 with the addition of SE [37], ECA [38], and CBAM attention mechanism modules. The results are presented in Table 1, indicating that the performance of YOLOv5 was significantly improved with the inclusion of the CBAM attention mechanism.

TABLE 2. Training data segmentation.

Number of edge servers	Train set	Training set partition ratio	Test set	Val set
1(C)	CPLID(Train)	1	CPLID(Test)	CPLID(Val)
2	CPLID(Train)	4:6	CPLID(Test)	CPLID(Val)
3	CPLID(Train)	2:3:5	CPLID(Test)	CPLID(Val)
4	CPLID(Train)	1:2:3:4	CPLID(Test)	CPLID(Val)
5	CPLID(Train)	1:1:2:2:4	CPLID(Test)	CPLID(Val)

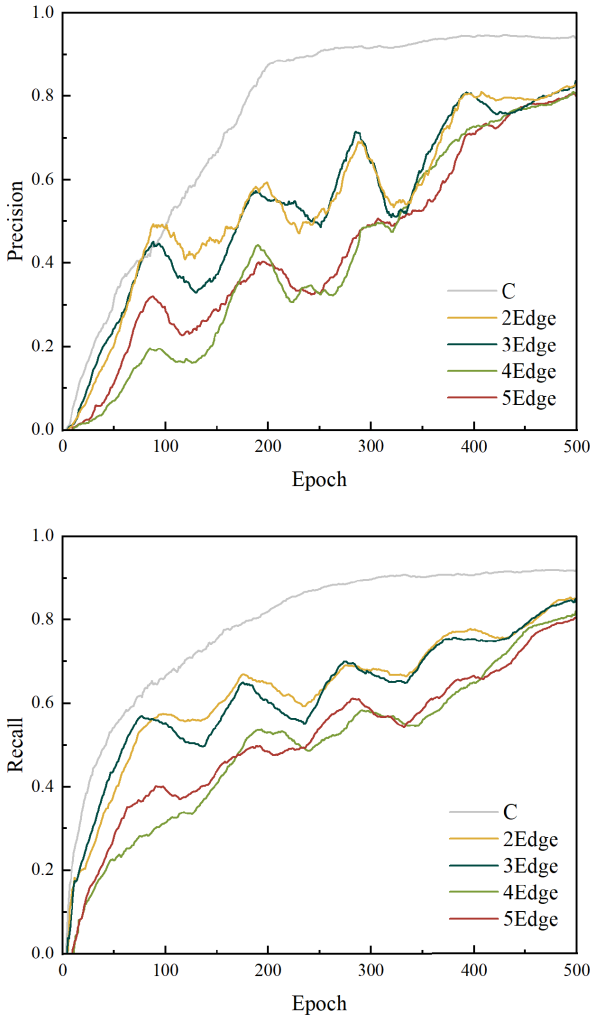

FIGURE 8. FL model performance.

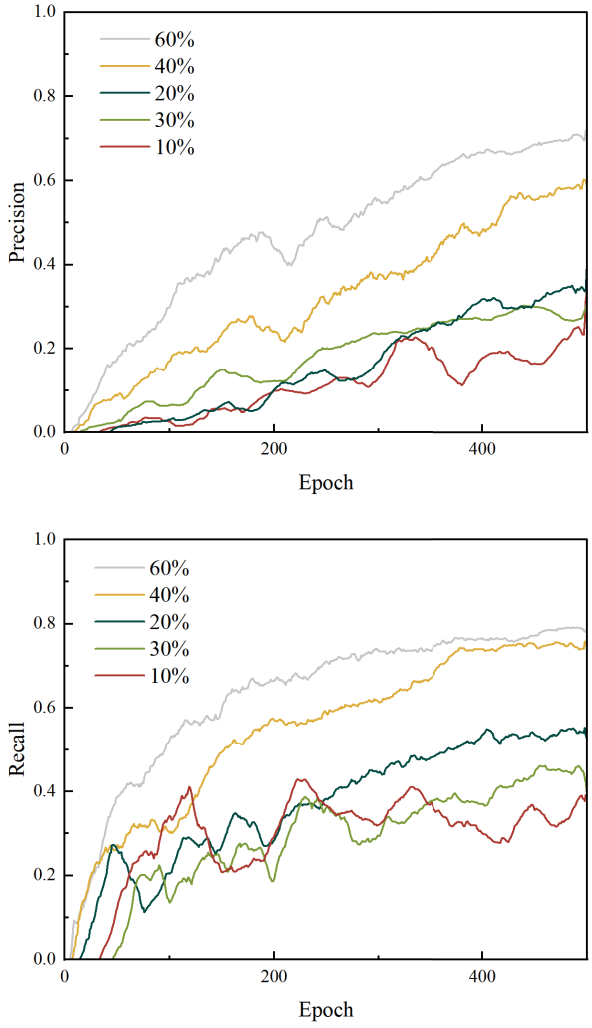

FIGURE 9. Performance of training models with different number of training sets.

D. FL BASED INSULATORS DETECTION MODEL

We employ the FedML-AI open source FL framework to implement Algorithm 1. Message Passing Interface(MPI) based parallel processing in FedML-AI effectively runs multiple processes simultaneously on a single workstation. We simulate a separate edge server for each process to conduct local sub-model training and thereby, simulate the DP-FedIOD training process. To ensure the effectiveness of our proposed method, we reorganized and redistributed the dataset, in varying proportions based on the number of edge servers present. This was done to replicate the non-uniform data distribution of each power operation unit in a realistic environment. To maintain consistency, the test and validation sets were adapted to the centralized training set. Table 2 shows the specific divisions of the data.

When there is only one edge server, it means that there is no parameter aggregation process, and centralized training is still performed. If the number of edge servers is two, the training set is divided and distributed in the ratio of 4:6. This holds true for the remaining cases listed in the table. The parameter settings used for centralized training in Section

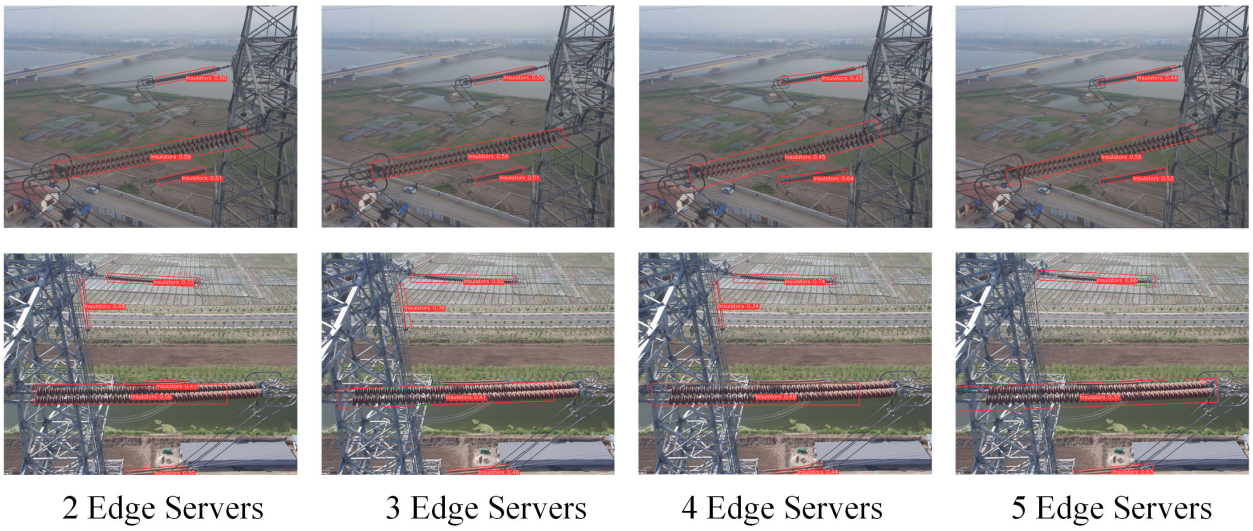

FIGURE 10. FL model validation results.

TABLE 3. FL model performance.

Number of edge serves	Precision/%	Recall/%
1(C)	95.00	92.30
2	83.28	85.81
3	82.78	83.27
4	81.10	81.81
5	80.30	80.90

IMPROVED YOLOV5 MODEL UNDER CENTRALIZED are also used, and the trained model is evaluated accordingly.

The precision and recall results are presented in Table 3 and their variation is shown in Figure 8. The analysis reveals that the precision and recall for models trained using FL are slightly lower compared to those obtained from centralized training. This outcome arises from the way in which the weighted average method aggregates parameters, leading to the discarding and blurring of some weight information. The accuracy of the trained models in distributed mode is above 79.06%, and the recall rate is above 80.16% with a consistent curve trend. Therefore, it can be concluded that the FL based method for insulator orientation detection is effective. Experiments were conducted on centralized training using varying numbers of training sets divided. The data volume of the original CPLID(Train) was divided into 10%, 20%, 30%, 40%, and 60% for centralized model training, and the Precision and Recall metrics were visualized. The results showed as Figure 9 that training with 10%, 20%, and 30% of the original data volume for centralized training did not produce models with high Precision and Recall values. Although using 40% and 60% of the data volume results in higher Precision and Recall values, they remain lower than those obtained from co-training the model on five edge servers, as illustrated in the figure above. This further confirms the efficacy of our proposed method in resolving the challenges faced by certain electric power companies in training accurate insulator detection models.

We have validated multiple model sets on the validation set, as indicated by the results shown in Figure 10. Our directed frames have accurately framed the insulators with high confidence.

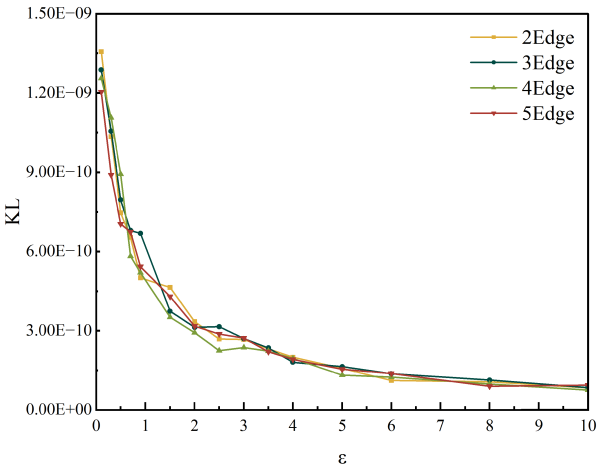

FIGURE 11. KL scatter curve.

TABLE 4. Performance of DP-FedIOD model with different values of ε.

ε=	0.1	0.3	0.5	0.7	0.9	1.5	2	2.5	3
Precision	64.6%	68.3%	71.2%	75.1%	76.9%	79.3%	79.9%	80.3%	80.7%
Recall	66.7%	69.1%	73.8%	76.5%	78.2%	81.2%	81.6%	81.9%	82.1%

E. VERIFYING THE PERFORMANCE OF DP-FEDIOD

To prevent privacy breaches during transmission of weight information for FL, we apply DP compliant Laplace noise to perturb the information uploaded from edge servers to cloud

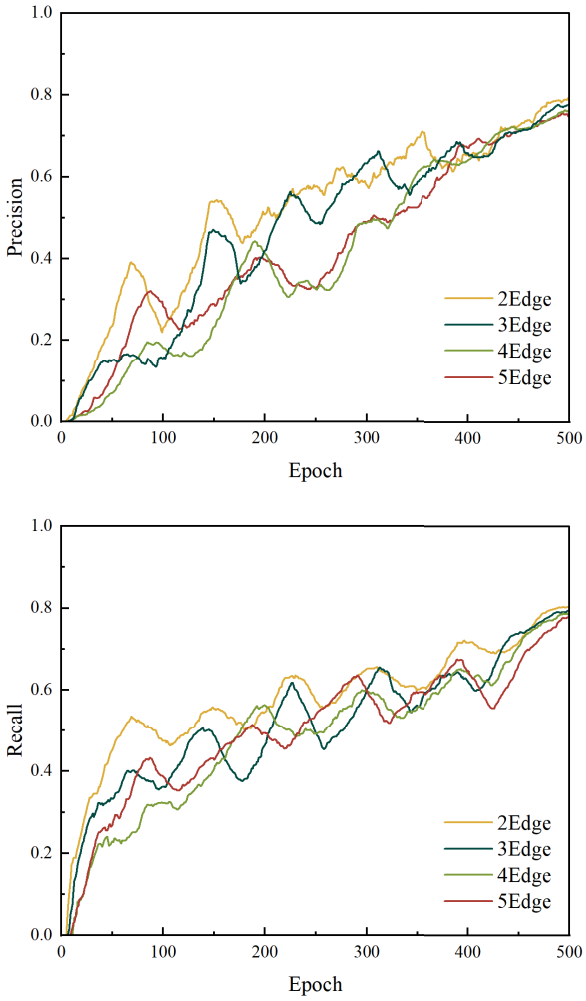

FIGURE 12. Model performance of DP-FedIOD at ε=1.5.

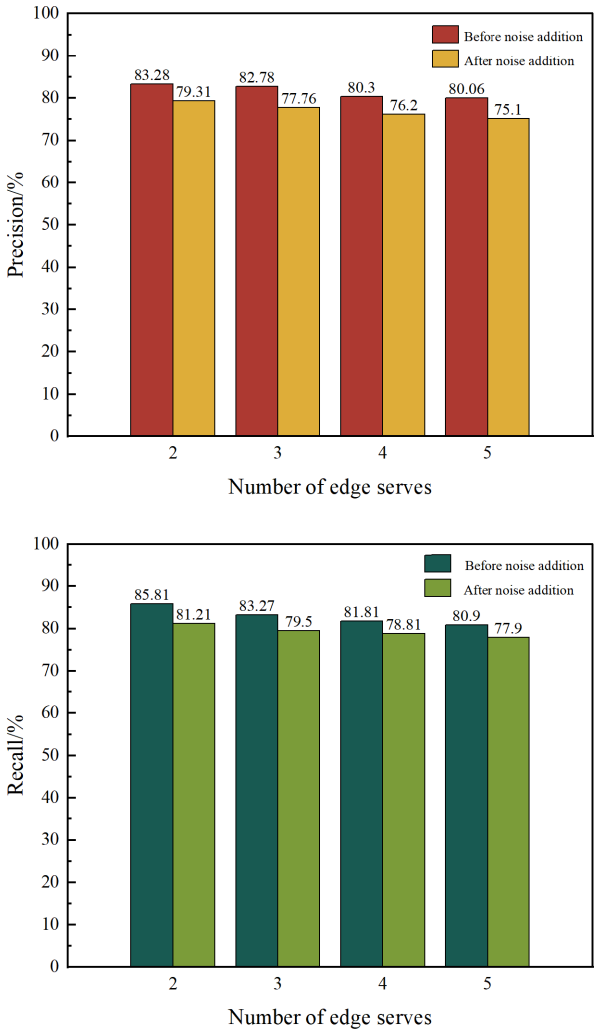

FIGURE 13. Comparison of collaborative model performance before and after noise addition.

servers. For model training under the federated structure of two edge servers, we first choose different values of ε. The global model precision and recall metrics obtained from the training are shown in Table 4. The precision and recall values of the trained global model are lower when the ε values are taken as 0.1, 0.3, 0.5, 0.7, indicating that the model performance is disrupted by noise. In contrast, the precision and recall values are higher and stabilized when the ε values are set to 0.9, 1.5, 2, 2.5, and 3, as illustrated in the Table 4.

In addition, we assess the effectiveness of preserving privacy by solving the KL divergence [39] for the weight information of the global model trained by varying numbers of edge servers, both pre- and post- the injection of different levels of noise. The KL scatter values of the models trained by various numbers of edge servers before and after adding noise are indistinguishable, as depicted in the Figure 11. Greater values of the privacy budget ε correspond to smaller KL scatter values and reduced privacy protection, whereas lesser values of ε lead to larger KL scatter values, indicating stronger privacy protection. This conforms to the definition of ε-differential privacy outlined in Section *DIFFERENTIAL PRIVACY*. When the value of ε exceeds 2, the KL scatter curve's decreasing trend becomes less drastic. This indicates that larger values of ε result in less disruptive information noise for model weights and subsequently weaker privacy protection. We would like to clarify that ε is used as a control variable for the amount of noise added during a single weight upload process. For the entire DP-FedIOD system, ε_{fed}-differential privacy is ensured, where $\varepsilon_{fed} = i \times \varepsilon$, i represents the number of weight uploads. This is in accordance with the serial and parallel combinatorial property for DP, based on the previously mentioned security analysis.

For optimal privacy preservation and model performance,, we determined that using Laplace noise with a privacy budget of $\varepsilon = 1.5$ was the optimal choice for our experiment on preserving privacy in FL models with varying numbers of edge servers. We visualized the precision and recall metrics of the global model. As depicted in Figure 12, the model is able

FIGURE 14. Detection effect of DP-FedIOD trained models.

to converge despite the perturbation of weight information by noise. After 500 epochs of training, the precision and recall values for various models are similar and above 75.10% and 77.90%, respectively. This indicates that the DP mechanism to preserve privacy when using FL based insulator detection models can be extended to scenarios involving a greater number of edge servers in training. In turn, this suggests that the proposed method has practical value for application. We compared the precision and recall metrics of FL models trained with varying numbers of edge servers before and after introducing noise. The results of the comparison are displayed in Figure 13. Following the introduction of Laplace noise that meets ε-differential privacy criteria during the training process, the precision and recall metrics of the model with noise perturbation were slightly lower compared to those of the noiseless model. Adding Laplace noise that complies with the ε-differential privacy mechanism to the uploaded weight information safeguards privacy data. However, during model training, weight information is subject to change, which negatively impacts model performance. This aligns with our expectations based on the DP theory.

Finally, we validate the detection of insulator images using the DP-FedIOD trained model. The results are presented in Figure 14, which demonstrate that the model achieves high accuracy for insulator recognition and localization. These results suggest that DP-FedIOD has the potential for real-world applications.

F. ANALYSE

The experiments demonstrate that DP-FedIOD is superior in detecting insulators. It accurately frames insulators with a rotating frame and achieves high detection speed and model accuracy. Additionally, DP-FedIOD solves the data silo problem in insulator detection through FL, providing a new solution for joint training of the global model. Finally, DP-FedIOD considers data privacy issues during the FL process. It employs a DP mechanism to mitigate the risk of differential attacks and model inversion attacks.

G. CHALLENGES OF REAL-WORLD DEPLOYMENT

The DP-FedIOD proposed here offers a novel solution to the problems of inaccurate identification of insulator locations and the difficulty of training DL models due to data silos faced by power operation units. Additionally, privacy requirements are taken into consideration. The experimental results demonstrate the feasibility and excellent performance of our method. However, some issues still need to be addressed before DP-FedIOD can be practically implemented for insulator detection in power operation units. The power operation units participating in DP-FedIOD must have the arithmetic capability to train a single sub-model. DP-FedIOD is a synchronous federated framework that requires all participants to upload the sub-model weights before the next step of aggregation. Additionally, the model detection performance is dependent on the data collected by the specific UAV device. These issues require further attention and consideration when deploying DP-FedIOD in the real world.

IV. CONCLUSION

Given the issue of imprecise positioning and data isolation in aerial insulator detection, we propose DP-FedIOD. This DP and FL based framework addresses the problem of data silos in real world insulator detection scenarios and also tackles the problem of imprecise localization of insulators and their defects, which are prevalent in existing insulator detection algorithms. And simulation experiments were conducted on CPLID, revealing that the improved YOLOv5 achieved an $mAP@0.5$ index of 95.00% with concentrated training. Without regard to privacy, it's precision and recall can both reach

80.30% and 80.90%, respectively, under the framework of distributed FL. Furthermore, DP-FedIOD exhibited precision and recall rates above 75.10% and 77.90%, respectively. Through these illustrations, the effectiveness and reliability of DP-FedIOD are evident. We believe that proposing DP-FedIOD is of practical significance for constructing an intelligent grid transmission and distribution insulation equipment monitoring system.

In future work, the focus will be on two main areas. Firstly, how to detect insulator defects under low resolution inspection images. Secondly, how to refine the selection of the privacy budget value in order to strike a balance between privacy preserving strength and model detection performance. Finally, the practical aspects of communication and hardware must also be taken into account when deploying DP-FedIOD in the real world.

REFERENCES

[1] K. P. Liu, B. Q. Li, and L. Qing, "A review on the application of deep learning target detection algorithm in overhead transmission line insulator defect detection," *High Voltage Technol.*, vol. 49, no. 9, pp. 3584–3595, 2022.

[2] Y. Zhai, R. Chen, Q. Yang, X. Li, and Z. Zhao, "Insulator fault detection based on spatial morphological features of aerial images," *IEEE Access*, vol. 6, pp. 35316–35326, 2018.

[3] Q. Wu, J. An, and B. Lin, "A texture segmentation algorithm based on PCA and global minimization active contour model for aerial insulator images," *IEEE J. Sel. Topics Appl. Earth Observ. Remote Sens.*, vol. 5, no. 5, pp. 1509–1518, Oct. 2012.

[4] Y. LeCun, Y. Bengio, and G. Hinton, "Deep learning," *Nature*, vol. 521, no. 7553, pp. 436–444, 2015.

[5] Y. Sui, P.-F. Ning, and P.-J. Niu, "A review of mountable UAV power inspection technology for overhead transmission lines," *Power Grid Technol.*, vol. 45, pp. 3636–3648, May 2021.

[6] R. Girshick, "Fast R-CNN," in *Proc. IEEE Int. Conf. Comput. Vis. (ICCV)*, Dec. 2015, pp. 1440–1448.

[7] S. Ren, K. He, R. Girshick, and J. Sun, "Faster R-CNN: Towards real-time object detection with region proposal networks," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 39, no. 6, pp. 1137–1149, Jun. 2017.

[8] K. He, G. Gkioxari, P. Dollár, and R. Girshick, "Mask R-CNN," in *Proc. IEEE Int. Conf. Comput. Vis. (ICCV)*, Oct. 2017, pp. 2980–2988.

[9] Q. Chen, B. Yan, R. Ye, and X. Zhou, "Research on aerial insulator convolutional neural network detection and self-detonation identification," *J. Electron. Meas. Instrum.*, vol. 31, no. 6, pp. 942–953, Jun. 2017.

[10] J. Zhong, Z. Liu, Z. Han, Y. Han, and W. Zhang, "A CNN-based defect inspection method for catenary split pins in high-speed railway," *IEEE Trans. Instrum. Meas.*, vol. 68, no. 8, pp. 2849–2860, Aug. 2019.

[11] G.-P. Liao, G.-J. Yang, W.-T. Tong, W. Gao, F.-L. Lv, and D. Gao, "Study on power line insulator defect detection via improved faster region-based convolutional neural network," in *Proc. IEEE 7th Int. Conf. Comput. Sci. Netw. Technol. (ICCSNT)*, Oct. 2019, pp. 262–266.

[12] Z. Ling, D. Zhang, R. C. Qiu, Z. Jin, Y. Zhang, X. He, and H. Liu, "An accurate and real-time method of self-blast glass insulator location based on faster R-CNN and U-Net with aerial images," *CSEE J. Power Energy Syst.*, vol. 5, no. 4, pp. 474–482, Dec. 2019.

[13] X. Tao, D. Zhang, Z. Wang, X. Liu, H. Zhang, and D. Xu, "Detection of power line insulator defects using aerial images analyzed with convolutional neural networks," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 50, no. 4, pp. 1486–1498, Apr. 2020.

[14] J. Redmon, S. Divvala, R. Girshick, and A. Farhadi, "You only look once: Unified, real-time object detection," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit. (CVPR)*, Jun. 2016, pp. 779–788.

[15] J. Redmon and A. Farhadi, "YOLO9000: Better, faster, stronger," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit. (CVPR)*, Jul. 2017, pp. 6517–6525.

[16] J. Redmon and A. Farhadi, "YOLOv3: An incremental improvement," 2018, *arXiv:1804.02767*.

[17] A. Bochkovskiy, C.-Y. Wang, and H.-Y. Mark Liao, "YOLOv4: Optimal speed and accuracy of object detection," 2020, *arXiv:2004.10934*.

[18] M. W. Adou, H. Xu, and G. Chen, "Insulator faults detection based on deep learning," in *Proc. IEEE 13th Int. Conf. Anti-Counterfeiting, Secur., Identificat. (ASID)*, Oct. 2019, pp. 173–177.

[19] X. M. Liu, H. Tian, and Y. M. Yang, "Research on image detection method of insulator defects under complex environment background," *J. Electron. Meas. Instrum.*, vol. 36, no. 2, pp. 57–67, 2022.

[20] S. Hao, L. Yang, and X. Ma, "Fault detection of YOLOv5 transmission line based on attention mechanism and cross-scale feature fusion," *Proc. CSEE*, vol. 43, no. 6, pp. 2319–2331, 2023.

[21] J. R. Zhang, X. Wei, L. X. Zhang, Y. N. Chen, and J. Lu, "Improved insulator detection and positioning for YOLOv7," *Comput. Eng. Appl.*, vol. 60, no. 4, pp. 1–11, Oct. 2024.

[22] Y. H. Huang, H. C. Liu, Z. Y. Chen, and J. R. Zhang, "Transmission line insulator fault detection based on USRNet with improved YOLOv5x," *High Voltage Technol.*, vol. 48, no. 8, pp. 3437–3446, 2022.

[23] D. L. Wang, S. H. Zhang, B. X. Yuan, W. B. Zhao, and R. Zhu, "Study on the detection of self-explosion defects in lightweight glass insulators based on improved YOLOv5," *High Voltage Technol.*, vol. 49, no. 10, pp. 4382–4390, 2023.

[24] H. B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. Y. Arcas, "Communication-efficient learning of deep networks from decentralized data," 2016, *arXiv:1602.05629*.

[25] 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 *Proc. AAAI Conf. Artif. Intell.*, 2020, pp. 13172–13179.

[26] C. He, A. D. Shah, Z. Tang, D. F. A. N. Sivashunmugam, K. Bhogaraju, M. Shimpi, L. Shen, X. Chu, M. Soltanolkotabi, and S. Avestimehr, "FedCV: A federated learning framework for diverse computer vision tasks," 2021, *arXiv:2111.11066*.

[27] C. He, S. Li, J. So, X. Zeng, M. Zhang, H. Wang, X. Wang, P. Vepakomma, A. Singh, H. Qiu, X. Zhu, J. Wang, L. Shen, P. Zhao, Y. Kang, Y. Liu, R. Raskar, Q. Yang, M. Annavaram, and S. Avestimehr, "FedML: A research library and benchmark for federated machine learning," 2020, *arXiv:2007.13518*.

[28] L. Sweeney, "Achieving k-anonymity privacy protection using generalization and suppression," *Int. J. Uncertainty, Fuzziness Knowl.-Based Syst.*, vol. 10, no. 5, pp. 571–588, Oct. 2002.

[29] C. P. Gupta and I. Sharma, "A fully homomorphic encryption scheme with symmetric keys with application to private data processing in clouds," in *Proc. 4th Int. Conf. Netw. Future (NoF)*, Oct. 2013, pp. 1–4.

[30] M. Abadi, A. Chu, I. Goodfellow, H. B. McMahan, I. Mironov, K. Talwar, and L. Zhang, "Deep learning with differential privacy," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, 2016, pp. 308–318.

[31] X. J. Zhang, F. C. He, J. Y. Gai, J. D. Bao, H. Y. Huang, and X. G. Du, "A differentially private federated learning model for fingerprinting indoor localization in edge computing," *J. Comput. Res. Develop.*, vol. 59, no. 12, pp. 2667–2688, 2022.

[32] A. Golatkar, A. Achille, Y.-X. Wang, A. Roth, M. Kearns, and S. Soatto, "Mixed differential privacy in computer vision," in *Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit. (CVPR)*, Jun. 2022, pp. 8366–8376.

[33] B. Zhao, H. Z. Ma, X. Zhang, C. L. Li, J. X. Zhao, X. J. Zhang, and Q. Zhang, "Research on directional identification of aerial insulators and its defect detection method," *J. Electron. Meas. Instrum.*, vol. 37, no. 5, pp. 240–251, May 2023.

[34] X. Yang and J. Yan, "On the arbitrary-oriented object detection: Classification based approaches revisited," *Int. J. Comput. Vis.*, vol. 130, no. 5, pp. 1340–1365, Mar. 2022.

[35] S. Woo, J. Park, J. Y. Lee, and I. S. Kweon, "CBAM: Convolutional block attention module," in *Proc. Eur. Conf. Comput. Vis. (ECCV)*, vol. 11211, 2018, pp. 3–19.

[36] Q. Yang, Y. Liu, T. Chen, and Y. Tong, "Federated machine learning: Concept and applications," *ACM Trans. Intell. Syst. Technol.*, vol. 10, no. 2, pp. 1–19, Mar. 2019.

[37] J. Hu, "Squeeze-and-excitation networks," 2017, *arXiv:1709.01507*.

[38] Q. Wang, B. Wu, P. Zhu, P. Li, W. Zuo, and Q. Hu, "ECA-Net: Efficient channel attention for deep convolutional neural networks," 2019, *arXiv:1910.03151*.

[39] H. Zhao, M. Xiao, J. Wu, Y. Xu, H. Huang, and S. Zhang, "Differentially private unknown worker recruitment for mobile crowdsensing using multi-armed bandits," *IEEE Trans. Mobile Comput.*, vol. 20, no. 9, pp. 2779–2794, Sep. 2021.

XUEJUN ZHANG received the M.S. degree from Southeast University, in 2009, and the Ph.D. degree from Xi'an Jiaotong University, in 2016. He is currently a Professor with Lanzhou Jiaotong University. His research interests include edge computing, differential privacy, cybersecurity, data privacy, and machine learning.

XIAO ZHANG received the B.S. degree from Southwest University, in 2021. He is currently pursuing the M.S. degree with Lanzhou Jiaotong University. His main research interests include object detection, federated learning, and differential privacy.

XIAOWEN SUN received the B.S. degree from Lanzhou Jiaotong University, in 2021, where he is currently pursuing the M.S. degree. His main research interests include federated learning and differential privacy.

FENGHE ZHANG received the B.S. degree from Shanxi University, in 2021. He is currently pursuing the M.S. degree with Lanzhou Jiaotong University. His main research interests include federated learning and natural language processing.

BIN ZHANG received the B.S. and M.S. degrees from China University of Petroleum and the Ph.D. degree from Harbin Institute of Technology. He is currently a Lecturer with Lanzhou Jiaotong University. His research interests include lidar and machine learning.

CHENGZE LI received the B.S. degree from Xidian University, in 2020. He is currently pursuing the M.S. degree with Lanzhou Jiaotong University. His main research interest includes federated learning.

XIAOHONG JIA received the B.S. degree from Shanxi Datong University, the M.S. degree from Lanzhou Jiaotong University, and the Ph.D. degree from Shaanxi University of Science and Technology. He is currently a Lecturer with Lanzhou Jiaotong University. His research interests include image segmentation and machine learning.