基于联邦学习的智能识别系统

熊子言[1] 蓝肖萍[1] 葛丽娜[1] 王 哲[1*]
XIONG Ziyan LAN Xiaoping GE Lina WANG Zhe

摘 要 随着深度学习的快速发展，目标检测算法得到了广泛应用，但是传统目标检测方法需要收集大量带标签的敏感数据，可能会侵犯用户隐私和数据机密性。联邦学习作为隐私保护分布式机器学习方法，可以实现端到端计算机视觉任务，其中图像注释和训练任务移动到边缘，而只有模型参数被发送到聚合服务器进行聚合。基于此，文章提出了一种基于联邦学习的边缘辅助物联网智能识别系统，该系统采用终端层、边缘服务层、网络层和云中心服务层的 4 层架构，可以分析物体分布的详细统计数据，以隐私保护的方式进行现实增强，辅助物联网设备进行安全且智能的物体识别。

关键词 智能识别；深度学习；物联网

doi：10.3969/j.issn.1672-9528.2025.09.041

0 引言

随着人工智能（artificial intelligence, AI）技术的飞速发展，机器学习、深度学习已经成为计算机视觉领域的核心技术[1]。机器学习主要目标是通过算法和模型从图像数据中提取有用的特征，并对图像进行分类、识别或分析，目前已用于人脸识别、物体检测与识别、图像分类、图像分割、图像生成、医学图像分析和智能交通等领域[2]。其中，深度学习[3]是机器学习的分支，主要基于人工神经网络模型，具有多层次的结构，在图像识别领域发挥了重要作用。图像识别是指从输入的图像数据中识别和分类出图像中的对象、场景或者特征。深度学习通过构建深层神经网络模型，利用大量的标注数据进行训练，从而实现对图像的高效识别[4]。在深度学习中，卷积神经网络（convolutional neural networks, CNN）是最常用的架构之一，适用于图像识别任务。CNN 能够有效地捕捉图像中的局部特征，并通过多层次的抽象表达来识别图像中的对象。通过反向传播算法，CNN 能够自动学习图像中的特征表示，并根据这些特征进行分类或识别。深度学习的不断发展和优化，使得图像识别在准确性和效率上都取得了巨大进步，为多领域带来了新的应用和解决方案[5]。然而，目前最先进的深度学习智能模型变得越来越庞大，其中包含数十亿甚至数万亿的可学习参数，高维的神经网络和额外的安全方案导致深度学习模型面临巨大的通信开销，成为深度学习模型规模扩大的主要瓶颈。同时，大多数传感器设备、网络存储设备等无时无刻不处理和存储海量数据，海量用户隐私数据的分布式存储导致人工智能模型很难利用各方数据和经验，并且难以保证模型共享过程中的隐私安全问题[6]。目前，制约深度学习技术在图像识别领域发展的短板涉及多个方面。

（1）数据安全：不可信的恶意敌手可能向参数聚合服务器发送错误的模型更新，以破坏模型精度。深度学习模型训练过程仍然涉及数据安全攻击的威胁，并有可能受到各种形式的攻击，如中毒攻击、后门攻击、搭便车攻击等。

（2）隐私泄露：恶意客户端或者半诚实学习方可能发起模型推断攻击以探测模型参数信息，从而推断本地数据集，造成本地隐私数据泄露。

（3）数据孤岛：目前的物联网传感设备收集的数据种类丰富，异构性强，且由于隐私安全问题，不同领域之间的数据共享性不高，数据整合程度较低，数据较为分散。不同领域之间的数据形成了“数据孤岛”，难以整合利用，不利于训练功能更加完善的深度学习模型。

为了有效解决机器学习、深度学习所面临的数据“孤岛”和隐私安全等问题，谷歌于 2016 年提出联邦学习（federated learning, FL）[7]。FL 作为一种在分布式边缘网络训练统计学习模型的范式，允许各参与者协作训练模型，而无需共享其本地数据，有效缓解了数据安全隐患，并打破数据“孤岛”[8]。FL 作为分布式机器学习方法，实现了源数据不出本地即进行全局模型训练。FL 可以更好地整合分散的数据资源，并进行深度分析，方便实时决策的制定和态势的感知，有效利用分散的数据资源，有助于图像识别领域的发展[9]。联邦学习已

1. 广西民族大学人工智能学院 广西南宁 530006
[基金项目] 广西自然科学基金（2024GXNSFAA010111、2025GXNSFBA069303）；广西高等教育本科教学改革工程项目（2022JGA163）

广泛应用于医疗保健[10]、智慧农业[11]、智能城市[12]、智慧工业[13]等领域。针对目前的基于深度学习的图像处理技术所面临的挑战，本文提出了一种基于联邦学习的边缘辅助物联网智能识别系统，主要工作内容如下：

首先，本文采用终端层、边缘服务层、网络层和云中心服务层4层架构设计了基于联邦学习的智能识别系统，以隐私保护的方式辅助物联网设备进行安全且智能的物体识别。其次，使用手写体图像MNIST数据集对本文所提的基于联邦学习的智能识别系统的有效性和准确性进行了实验验证和分析。结果表明，本文所提系统可以用隐私保护的方式实现较高的模型准确率。

1 FL概述与相关技术

1.1 FL定义

联邦学习旨在建立一个分布数据集的联邦学习模型。此场景下，云端参数服务器作为协调方，可以将初始模型发送给N个参与方，各个参与方分别使用各自的训练数据集$\{D_i\}_{i=1}^{n}$协作训练机器学习模型，并将模型权重更新参数加密上传至参数服务器，参数服务器再将接收到的模型聚合起来，聚合的方法可以是联邦平均算法。之后，参数服务器会将聚合后的模型更新发回给参与方。这一过程将反复执行，直至模型收敛或者达到最大迭代次数。联邦学习架构可以被设计为对等网络的方式。这种架构下的各参与者处于对等地位，无主从之分，每个参与者既可以作为模型训练方，为其他参与方提供模型参数，参与联邦建模和联邦推理。又可以作为业务方，发起业务场景的联邦建模和联邦推理。这种架构消除了单点故障问题带来的隐患，进一步确保系统安全，且易于扩展，但可能消耗较多的计算资源在消息通信的加密和解密[14]。

1.2 FL分类

假设第m个参与方的数据用矩阵$\boldsymbol{D}_m$表示，矩阵$\boldsymbol{D}_m$的每一行表示一个数据样本，每一列表示一个具体的数据特征。对于有标签信息的数据集，假设特征空间为X，数据标签空间为Y，样本ID空间为I。根据训练数据在不同参与方之间的数据特征空间和样本ID空间的分布情况，联邦学习被划分为横向联邦学习、纵向联邦学习和联邦迁移学习。

1.2.1 横向联邦学习

横向联邦学习适用于参与方的数据特征重叠较多的情况。如表1所示，当联邦学习的参与方A和参与方B是两家不同的银行时，且只有较少的重叠客户，但不同客户$I_1, I_2,\cdots, I_n$的数据可能因为相似的商业模式而有非常相似的特征空间，即两家银行的用户重叠部分较小，但数据特征的重叠部分较大，两家银行可以通过横向联邦学习来协同建立一个机器学习模型。因此，横向联邦学习也被称为按样本划分的联邦学习。

表1 横向联邦学习

	ID	X_1	X_2	X_3	Y
参与方A	I_1				
	I_2				
参与方B	I_3				
	I_4				

1.2.2 纵向联邦学习

纵向联邦学习的特点是参与方之间的数据样本是对齐的，但是在数据特征上有所不同。如表2所示，参与方A和参与方B提供不同的服务，但在客户群体上有非常大的交集时，他们可以在各自的不同特征空间上协作，为各自得到一个更好的统计学习模型。由于用户之间的重叠部分较大，但数据特征重叠部分较小。因此，纵向联邦学习也被称为按特征划分的联邦学习。

表2 纵向联邦学习

参与方A	ID	X_1	X_2	Y	参与方B	ID	X_3	X_4	Y
	I_1								
	I_2								

1.2.3 联邦迁移学习

联邦迁移学习允许在数据联合中跨域传输互补知识，通过对现有模型结构进行较小的修改，帮助只有少量数据（较少重叠的样本和特征）和弱监督（较少标记）的应用建立有效且精确的机器学习模型。尤其是在医疗、智能制造、数据预测、图形图像处理等这种数据异构性特别强烈的应用领域。联邦迁移学习基于分布在多方的数据来建立模型，是针对不同参与方的数据不仅样本空间不同而且特征空间也不同的情况而设定的，适用于联邦学习参与方的数据样本和数据特征重叠都很少的情况。在联邦学习体系中融入迁移学习可能在很大程度上解决迁移学习应用的局限性，对联邦学习体系的完善和发展是非常有利的。联邦迁移学习的特点是参与方的数据样本和数据特征重叠都很少。联邦迁移学习基于分布在多方的数据来建立模型，并且各方的数据都无法集中到一起或者提供给其他方。联邦迁移学习被用于解决数据量不足以及样本标签数少的问题。如表3所示，参与方A和参与方B之间的用户实体和相关的数据特征存在较大区别。不同企业之间的数据交流和整合利用是非常困难的，但迁移联邦学习的提出，为解决此类问题提供了良机。如今，异构性问题仍然是联邦环境中的关键挑战，动态多源异构数据在样本维和特征维存在很小的交集，异构网络下的联邦迁移学习框架，在保证隐私安全的同时，保证了联邦学习的模型精

度和训练效率。

表 3 联邦迁移学习

参与方 A	ID	X_1	X_2	Y				
	I_1							
	I_2							
					参与方 B	ID	X_3	X_4	Y
						I_3			
						I_4			

1.3 相关技术

1.3.1 分布式深度学习

统计学习模型的训练需要大量数据且过程复杂。随着模型训练的进行，输入模型的训练数据渐增，参数数量也会渐增，导致整个机器学习过程消耗大量资源，如硬件存储、处理资源等。为此，提出分布式学习实现数据并行、模型并行。分布式学习利用多个计算节点进行统计模型训练旨在提高模型训练性能、保护隐私。分布式机器学习使用分布式资源进行训练，解决单台机器上无法处理大规模数据训练的问题。分布式机器学习利用数据并行，模型并行和管道并行来并行化训练过程，显著加快了机器学习训练速度，减少训练时间。其中，深度学习作为机器学习先进的方法之一，能够从大量复杂数据中学习样本数据的内在规律和表示层次，但在某些无法提供足够标记训练数据集的领域，深度学习性能将大打折扣。分布式深度学习作为主流的解决方案，利用多个数据源进行模型训练，从大型和多样的数据集中获益。然而，大多数参与学习的实体往往分布在各个领域，由于行业规则、法律政策及隐私问题等原因，并不愿意无偿贡献自己的私有数据。因此，分布式深度学习处理敏感领域的隐私数据时，不仅要注重模型可用性，更要注重敏感数据隐私安全。FL 作为一种分布式机器学习方法，分布式客户端协作训练机器学习模型，同时保持原始数据留存本地，无需集中到单一服务节点，不仅充分利用了分布式资源，也为去分布式客户端私有数据提供隐私安全保证。

1.3.2 卷积神经网络

卷积神经网络作为一种深度学习模型，专门用于处理图像和视频等具有网络结构的数据，卷积神经网络技术在图像识别和计算视觉任务发挥重要作用。典型的卷积神经网络结构包括多个交替的卷积层和池化层，以及最终的全连接层。常见的模型包括 LeNet、AlexNet、VGG、GoogLeNet、ResNet 等，根据网络深度、参数数量和任务复杂度不同而有所区别。卷积神经网络中的卷积操作是指将一个可移动的卷积核进行逐元素相乘然后再相加的操作，卷积神经网络的结构如图 1 所示，主要分为 4 层，分别是输入层、卷积层、池化层以及全连接层，每层具体工作原理如下：

（1）输入层用于接收具有网络结构的数据，比如图像和视频。相较于传统典型的人工神经网络将矩阵数据转化为一维数据形式，卷积神经网络保留了图像数据的空间相关性。其中，图像通常由 3 个颜色通道组成（红、蓝、绿）。

（2）卷积层是卷积神经网络的核心组成部分，通过卷积操作从输入图像中提取特征。卷积操作通过滤波器（也称为卷积核）在输入图像上滑动，每次计算滤波器与图像区域的点乘积，生成特征图（也称为特征映射）。这些特征图捕捉了图像中的局部特征，如边缘、纹理等。

（3）池化层用于减少特征图的空间维度，同时保留最重要的特征信息。常见的池化操作包括最大池化（Max Pooling）和平均池化（Average Pooling），分别取池化窗口中的最大值或平均值作为输出。

（4）在卷积神经网络的顶部，通常会连接一个或多个全连接层，将卷积层提取的特征进行分类或回归预测。全连接层的输出通过 softmax 函数（用于分类问题）或者线性激活函数（用于回归问题）转换成最终的预测结果。

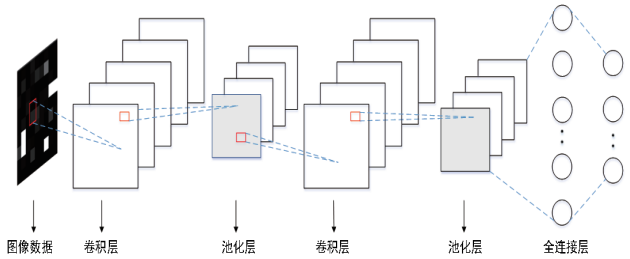

图 1 卷积神经网络结构图

2 基于联邦学习的手写体图像识别

2.1 网络模型

为解决深度学习中使用额外的安全方案导致的巨大通信开销、分布式异构数据难以整合利用，以及难以保证模型共享过程中的隐私安全等问题。本文结合联邦学习的分布式隐私保护学习方式设计了基于联邦学习的智能识别系统。该系统主要由四层网络架构，如图 2 所示，自下而上分别是终端层、边缘服务层、网络层和云服务层。首先，通过终端层收集的图像数据会上传至边缘服务层，然后，边缘服务层中的多个边缘计算节点会对收集的图像数据执行一轮或者多轮本地模型训练，其次，边缘计算节点将训练好的本地模型参数通过网络层的安全信道传输至云服务层，最后，云服务层对收集到的所有本地模型参数执行全局模型聚合，并判断全局模型精度是否达到设定阈值，如果达到，则停止训练，如果没有，云服务层作为联邦学习的聚合中心，会将本轮训练的全局模型经由网络层下发给边缘计算节点，然后继续模型训练。

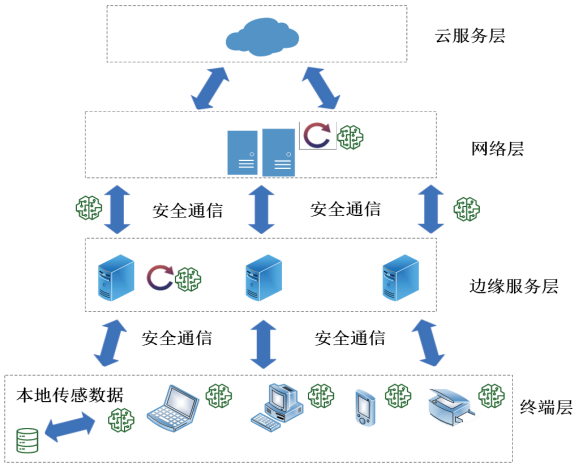

图 2 联邦学习的边缘辅助物联网智能识别系统

各层主要功能介绍如下：

（1）终端层：终端层包括各种物联网设备、传感器、智能手机和其他智能终端设备。这些设备负责采集和生成数据，并进行初步处理。例如，温度传感器可以直接读取温度数据，智能相机可以捕捉视频图像。同时，终端层可以对原始数据进行预处理和过滤，减少冗余信息，降低数据传输量。例如，视频监控摄像头可以在本地对视频数据进行压缩，或者仅上传涉及异常活动的片段，而不是整个视频流。最后，终端层可以提供初步的安全措施，如数据加密、身份验证等，确保数据在传输和存储过程中的安全性和隐私保护。例如，医疗设备可以在本地加密患者数据，再上传至边缘或云端。

（2）边缘服务层：边缘服务层位于终端层和网络层之间，由若干边缘计算节点组成，负责协调和管理多种边缘终端设备的本地训练任务。边缘服务层中的计算节点可以对收集的边缘终端设备的本地数据进行本地聚合模型更新，进行本地模型优化，并向云服务层发送聚合后的本地模型更新。同时，由于边缘服务层靠近终端设备数据源，可以实现低延迟的实时响应，并可以提供初步的安全措施，比如身份验证、访问控制、数据加密等，确保数据传输和存储过程的隐私性和安全性。

（3）网络层：网络层负责边缘终端设备、边缘服务器和云服务器之间的数据传输和模型更新，主要包括从边缘计算节点和高性能终端设备上传本地模型更新至云服务层执行全局模型聚合、云服务器向边缘计算节点或设备下发全局模型等。网络层使用安全传输协议对传输的模型参数进行数据加密，防止数据窃听和篡改。同时，网络层也通过动态调整传输频率和数据量，平衡模型更新的及时性和网络负载，管理和优化带宽的使用。

（4）云服务层：云服务层作为整个系统的中央协调节点，负责管理和协调联邦学习过程中的各项任务。云服务层负责初始化全局模型，将初始模型参数发送到所有参与的边缘服务器和边缘设备。这是联邦学习的起始步骤，确保所有设备都从相同的模型开始训练。同时，云服务层接收来自各个边缘服务器的聚合模型更新（如梯度或模型参数），进行全局聚合。这通常包括加权平均，将各边缘设备的贡献合并成一个更新后的全局模型。最后，云服务层将聚合后的全局模型参数分发回边缘服务器，然后由边缘服务器进一步分发给各个边缘设备，进行下一轮本地训练。这个过程在每一轮联邦学习迭代中重复进行，直到模型收敛。

2.2 基于联邦学习的智能识别模型训练

为了解决传统隐私安全方案带来的巨大通信开销，保证模型共享过程中的隐私安全问题，本文系统使用联邦学习设计了智能识别系统，使用集中式联邦学习架构解决传统深度学习需要上传原始本地数据至中心服务器进行训练的问题，避免了原始数据的直接泄露。同时，联邦学习架构允许多方数据源协同合作，缓解了异构数据难以利用的问题。基于联邦学习的智能识别模型训练流程如下：

（1）全局初始化：云服务中心初始化全局模型，并通过网络层的安全信道进行传输，分发给所有边缘计算服务器，再由边缘服务器分发给各个可以独立进行本地模型训练的边缘终端设备。

（2）本地模型训练：每个高性能终端设备会使用本地的数据集进行全局模型训练，并计算模型更新。对于部分性能有限的边缘终端设备，则需要将本地数据上传至就近的边缘计算服务器执行一轮或多轮的本地模型训练。

（3）本地模型更新上传：高性能边缘终端设备和边缘计算服务器会使用差分隐私技术对本地模型更新进行加噪，然后上传至云中心服务器进行全局模型聚合。

（4）全局模型聚合：云中心服务器将接收到的加密后的本地模型更新执行全局聚合，并更新全局模型，本文系统采用的是联邦平均聚合算法来聚合全局模型。

（5）模型分发：云中心服务器判断当前的全局模型将更新后的全局模型下发到边缘服务器，再由边缘服务器分发到边缘设备，进入下一轮迭代，直到模型收敛。

3 实验结果与分析

为验证本文所提的基于联邦学习的智能识别系统的有效性，本节设置了仿真实验，验证所提系统在 MNIST 数据集上的有效性，以及在不同隐私预算下的模型准确性进行讨论和评估，并设计对比实验验证本文所提系统的先进性。

3.1 实验环境设置

本文实验环境配置如下：Intel(R) Core(TM) i7-9700 CPU @ 3.00 GHz，32 GB 内存，Windows11 操作系统。实验使用 TensorFlow 2.0 搭建 FL 框架，并采用 CNN 作为训练模型。

3.2 数据集

本文使用真实环境下采样生成的 MNIST 手写体图像数据集对本文所提系统的有效性进行验证。MNIST 数据集是机器学习和计算机视觉领域的重要基准数据集，广泛用于手写数字识别任务，MNIST 数据集由 60 000 个训练样本和 10 000 个测试样本组成。每个样本是一个像素为 28 px×28 px 的灰度图像，代表手写的 0~9 之间的一个数字。数据集由美国国家标准与技术研究所（NIST）提供。MNIST 数据集中均为 28 px×28 px 大小的灰度图像，每个像素的值在 0 到 25 之间，表示不同的灰度等级。其中，每个图像都有一个对应的标签，表示图像中的数字（0~9），标签是整数，共有 10 个类别。为了构造真实的分布式学习场景，本节实验共设置了 10 个客户端设备，并将整个 MNIST 数据集随机划分为 10 等份，每份子集分别发送给一个客户端设备进行本地模型训练。

3.3 超参数设置和评估指标

本节实验超参数设置全局迭代次数为 100，客户端节点本地训练轮数为 3，学习率为 0.005，MNIST 数据集本地训练批次大小为 10，本地训练采用随机梯度下降优化算法。

本节实验使用准确率和精确率两个指标来评估模型的性能，计算公式分别为：

$$\text{Accuracy} = \frac{TP+TN}{TP+TN+FP+FN} \tag{1}$$

$$\text{precision} = \frac{TP}{TP+FP} \tag{2}$$

式中：TP 为真阳性；TN 为真阴性；FP 为假阳性；FN 为假阴性。

3.4 实验结果对比

为验证本文所提基于联邦学习的智能识别系统的有效性，本节实验在 MNIST 数据集上对本文所提系统与方案 1[15]、方案 2[16] 的模型准确性进行了对比。其中，方案 1 和方案 2 均使深度学习训练图像识别模型，并未增加额外的隐私安全方案。由图 3 可知，本文所提系统方案的模型准确率高达 98.7%，对比方案 1 和方案 2 的模型准确率高，证明了本文所提的基于联邦学习的智能识别系统的有效性。

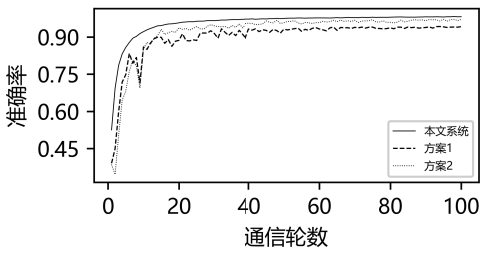

图 3 不同方案的模型准确率对比

表 4 统计了本节实验对比了不同方案在 MNIST 数据集上取得的模型准确率和精度，本文所提系统在增加了额外的隐私安全机制后仍取得了最高的模型准确率，比对比方案 2 高 1.6%，而对比方案 1 和方案 2 则没有添加额外的隐私安全机制，本地数据上传至中央服务器执行训练任务的过程存在着严重的数据安全问题和隐私泄漏风险。恶意敌手可以攻击中央服务器对模型参数进行篡改，破坏模型精度，或者在训练过程中窃取本地用户原始数据集信息。由于深度学习模型的训练需要大量的用户数据，一旦中央服务器被恶意敌手攻陷或者与其勾结都有可能导致大规模的隐私数据泄露或者模型精度受损，对用户造成巨大损失。而本文所提系统仅需要上传本地模型更新至云中心服务器进行全局模型训练，用户原始数据留存本地，有效缓解了用户本地隐私数据泄露的风险。同时，本文所提系统采用差分隐私技术对本地模型更新进行了加噪处理，保证其在传输过程和全局模型聚合中的隐私安全性，即使恶意敌手获取加噪后的本地模型更新，也无法准确推断用户原始隐私数据。此外，由于不同客户端拥有的数据分布不同，可能巨大的样本量训练的模型准确率反而不高，并且部分客户端由于隐私安全问题并不愿意主动贡献自己的本地数据参数模型训练。本文所提系统使用联邦学习训练范式，以隐私保护的方式协作训练全局模型，有效打破了“数据孤岛”，可以协同训练多方数据。

表 4 不同方案的准确率和精度的对比结果

数据集	对比方案	准确率 /%	精度 /%
MNIST	本文方案	98.7	99.2
	方案 1	93.7	95.5
	方案 2	97.1	98.9

基于联邦学习的智能识别系统在边缘计算服务器上传本地模型参数之前会使用基于拉普拉斯噪声扰动的差分隐私技术对本地模型参数进行加噪保密，然而局部差分隐私的设置可能对本地模型参数和全局模型的准确性产生一定的影响。因此，本节实验对不同隐私预算下的联邦学习全局模型准确性进行了统计验证和对比，并给出了隐私预算参数讨论的过程。图 4~7 分别统计了不同的隐私预算设置对联邦学习全局模型准确率的影响。

图 4 实验结果显示了不添加任何隐私噪声情况下的联邦学习全局模型准确率，不添加隐私策略的传统联邦学习模型在第 100 轮通信的时候模型准确性稳定 98% 左右，此时模型性能较优。其中，图 5~7 分别统计了添加隐私噪声保护客户端本地模型更新时的联邦学习全局模型的准确率。可以看出使用局部差分隐私技术保护客户端本地模型参数的时候，全局模型的准确率会有影响，准确率有所下降，而且不同的隐

私预算设置下，模型的收敛速度和达到稳定后的模型准确率也是有所不同。

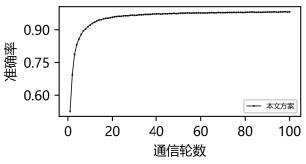

图 4 未添加隐私噪声的全局模型准确率

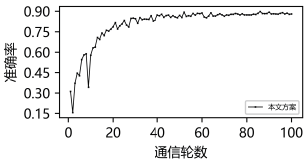

图 5 全局模型准确率（隐私预算设置为 2.5）

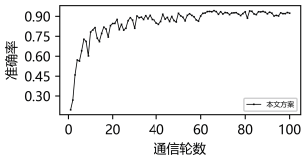

图 6 全局模型准确率（隐私预算设置为 3.0）

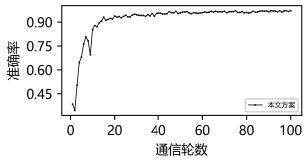

图 7 全局模型准确率（隐私预算设置为 3.5）

图 5 所示，在隐私预算设置为 2.5 的时候，全局模型准确率最高达到 89.2%。在训练初期，由于添加了拉普拉斯噪声保护本地模型参数隐私性，此时模型准确率出现波动，并不稳定，随着训练轮数增加，模型准确率逐渐趋于稳定，100 轮训练时最高达到 89.2% 的模型准确率。图 6 显示了隐私预算设置为 3.0 时的全局模型准确率，100 轮训练后的模型准确率逐渐稳定，最高达到 91.8%。图 7 显示了隐私预算设置为 3.5 时的全局模型准确率，100 轮训练后的模型准确率最高达到 94.2%。

表 5 统计了不同隐私预算设置下的联邦学习全局模型准确率，随着隐私预算的增加，全局模型的准确率也在提高，这是因为隐私预算和噪声比例设置不同而引起的，越高的隐私预算，则添加的噪声越少，对模型准确率的影响越小，因此可以在不过多地影响模型准确率的情况下可以起到隐私数据保护的作用。同时，噪声如果添加太少，则隐私保护的效果也不好。

表 5 不同隐私预算设置的模型准确率对比结果

隐私预算	准确率 /%
未添加噪声	98.2
2.5	89.2
3.0	91.8
3.5	94.2

4 结论

本文提出了一种基于联邦学习的边缘辅助物联网智能识别系统，基于终端层、边缘服务层、网络层和云中心服务层的四层架构设计了基于联邦学习的智能识别系统，以隐私保护的方式辅助物联网设备进行安全且智能的物体识别。其次，本文对基于联邦学习的智能识别系统的有效性和准确性进行了实验验证和分析，结果表明，本文所提系统可以用隐私保护的方式实现较高的模型准确率。但差分隐私技术的使用仍然在隐私性和有效性之间存在平衡问题，后续研究将进一步改进使用差分隐私技术，在保护模型隐私性的同时对模型准确性的影响减小。

参考文献：

[1] BAYOUDH K. A survey of multimodal hybrid deep learning for computer vision: architectures, applications, trends, and challenges[J]. Information fusion, 2024,105: 102217.

[2] SAINI M, SUSAN S. Tackling class imbalance in computer vision: a contemporary review[J]. Artificial intelligence review, 2023, 56(l1): 1279-1335.

[3] LECUN Y, BENGIO Y, HINTON G. Deep learning[J]. Nature, 2015, 521(7553): 436-444.

[4] MENGHANI G. Efficient deep learning: a survey on making deep learning models smaller, faster, and better[J]. ACM computing surveys, 2023, 55(12): 1-37.

[5] 窦慧 , 张凌茗 , 韩峰 , 等 . 卷积神经网络的可解释性研究综述 [J]. 软件学报 , 2024, 35(1): 159-184.

[6] KHOEI T T, SLIMANE H O, KAABOUCH N. Deep learning: systematic review, models, challenges, and research directions[J]. Neural computing and applications, 2023, 35(31): 23103-23124.

[7] MCMAHAN H B, MOORE E, RAMAGE D, et al. Communication-efficient learning of deep networks from decentralized data[EB/OL].(2023-01-26)[2024-05-12].https://doi.org/10.48550/arXiv.1602.05629.

[8] 肖雄 , 唐卓 , 肖斌 , 等 . 联邦学习的隐私保护与安全防御研究综述 [J]. 计算机学报 ,2023,46(5):1019-1044.

[9] KHOKHAR F A, SHAH J H, KHAN M A, et al. A review on federated learning towards image processing[J]. Computers and electrical engineering, 2022, 99: 107818.

[10] CHADDAD A, WU Y H, DESROSIERS C. Federated learning for healthcare applications[J]. IEEE internet of thingsjournal, 2023, 11(5): 7339-7358.

[11] MUHAMMED D, AHVAR E, AHVAR S, et al. Artificial intelligence of things (AIoT) for smart agriculture: a review of architectures, technologies and solutions[J]. Journal of network and computer applications, 2024,228: 103905.

[12] PANDYA S, SRIVASTAVA G, JHAVERI R, et al. Federated learning for smart cities: a comprehensive survey[J]. Sustainable energy technologies and assessments, 2023, 55: 102987.

油气管道无人机巡检中通信技术优化与应用研究

唐经纶[1]
TANG Jinglun

摘 要 利用无人机进行巡线作业对油气管道运输在提升管道巡检效率、保障作业安全的同时，也能够促进系统自动化与智能化发展，完成智慧站场互联。为充分探讨无人机通信技术给管道巡检带来的优势，文章介绍了当前油气管道巡检的现状，对比了无人机巡检代替有人巡检队伍的优劣，对油气管道无人机巡检作业中涉及的数据传输方式进行了阐述。针对当前无人机管道巡检技术中普遍存在的通信技术的瓶颈与挑战，结合目前已经建设的无人机巡检工程项目，研究并展开分析了无人机通信技术的优化对巡线效率、检测成本、作业安全等方面的关键提升，并对无人机巡线的应用前景进行了展望。

关键词 无人机；管道巡检；无线通信；技术优化

doi：10.3969/j.issn.1672-9528.2025.09.042

0 引言

油气管道是当前能源储运的重要组成部分，其将石油天然气等化石燃料从上游输送至下游，以供交通运输、合成原料、工农业生产、居民用能等所需，因此被誉为能源运输的大动脉。国际能源署发布的《全球能源评论 2025》报告指出，2024 年全球能量需求增长速度快于过去十年平均水平，对所有燃料和技术的需求都将扩大，2024 年天然气和石油的全球需求与 2023 年同比增长了 2.7% 和 0.8%，中国天然气需求增长量最大（如图 1 所示），增长超过 7%（3×10^{10} m^3）。

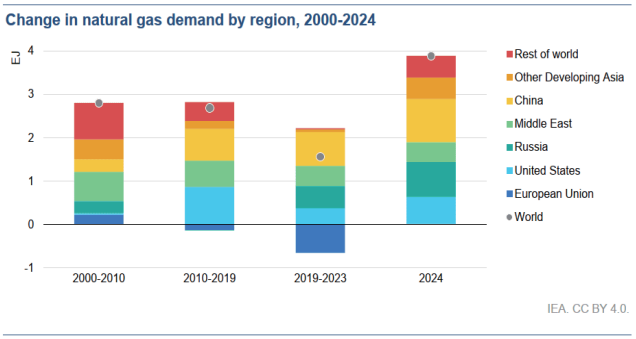

图 1 2000—2024 年区域天然气需求变化

（摘自《全球能源评论 2025》报告）

在全球能源体系背景下，石油天然气的能源地位短期

1. 国家管网集团工程创新有限公司华东设计院
江苏徐州 221008

[13] ZHOU J H, LU Q H, DAI W B, et al. Guest editorial: federated learning for industrial IoT in industry 4.0[J]. IEEE transactions on industrial informatics, 2021, 17(12): 8438-8441.

[14] LI H A, GE L H, TIAN L. Survey: federated learning data security and privacy-preserving in edge-Internet of things[J]. Artificial intelligence review, 2024, 57(5): 130.

[15] LUO J. Research on image recognition methods based on deep learning[J].Journal of physics: conference series,2019,1395:25-27.

[16] ZHANG H Q, LI J, LIU S Q, et al. A human body infrared image recognition approach via DCA-Net deep learning models[J]. International journal on artificial intelligence tools, 2023, 32(5): 2360004.

【作者简介】

熊子言（2004—），男，广西玉林人，本科，研究方向：联邦学习。

蓝肖萍（2002—），女，广西河池人，本科，研究方向：联邦学习、车联网和无线携能通信。

葛丽娜（1969—），女，广西环江人，博士，教授、硕士生导师，研究方向：计算机网络与信息安全。

王哲（1991—），通信作者（email:designbyyili@163.com），男，河南南阳人，博士，副教授、硕士生导师，研究方向：计算机网络、携能通信与智能算法。

（收稿日期：2025-03-04 修回日期：2025-08-29）