融合边缘智能计算和联邦学习的隐私保护方案

刘 东[1]，裴锡凯[2]，赖金山[3]，王瑞锦[3*]，张凤荔[3]

(1. 电子科技大学计算机科学与工程学院 成都 611731；2. 成都民航空管科技发展有限公司 成都 610042；
3. 电子科技大学信息与软件工程学院 成都 610054)

【摘要】边缘智能设备、网关和云端在智能协同计算的过程中，存在隐私泄露、计算能力有限等问题。提高联邦学习可以大大提高智能协同计算的训练效率，但也会暴露边缘智能终端的训练集信息。基于此，提出了一种融合边缘智能计算和联邦学习的隐私保护方案 (PPCEF)。首先，提出了一个基于共享秘密和权重掩码的轻量级隐私保护协议，该协议基于秘密共享的随机掩码方案，不仅可以在不损失模型精度的前提下保护梯度隐私，还可以抵抗设备掉线和设备间的共谋攻击，具有很强的实用性。其次，设计一种基于数字签名和哈希函数的算法，不仅可以实现消息的完整性和一致性，还能抵抗重放攻击。最后，使用 MNIST 和 CIFAR10 数据集，证明提出的 PPCEF 方案在实践中安全且高效。

关 键 词 智能协同计算； 边缘网关； 联邦学习； 隐私保护
中图分类号 TP181; TP391.1 **文献标志码** A doi:10.12178/1001-0548.2022176

Privacy Protection Scheme Combining Edge Intelligent Computing and Federated Learning

LIU Dong[1], PEI Xikai[2], LAI Jinshan[3], WANG Ruijin[3*], and ZHANG Fengli[3]

(1. School of Computer Science and Engineering, University of Electronic Science and Technology of China Chengdu 611731;
2. Chengdu Civil Aviation Air Traffic Control Technology Development Co., Ltd. Chengdu 610042;
3. School of Information and Software Engineering, University of Electronic Science and Technology of China Chengdu 610054)

Abstract Edge intelligent computing is widely used in the fields of Internet of things (IoT), industrial control UAV cluster and so on, which has the advantages of high data processing efficiency, strong real-time performance and low network delay. However, there are many problems when edge intelligent device, edge gateways and cloud complete the task unloading, scheduling and coordination. For example, there are problems that are privacy disclosure, limited calculation force. As is known to all, federated learning allows all training devices to complete training in parallel, which greatly improve training efficiency. However, traditional federated learning will expose the edge device's information of the training set. So, this article propose a privacy protection scheme combining edge intelligent computing and federated learning (PPCEF). First of all, we propose a lightweight privacy protection protocol based on sharing secret and weight mask, which is based on a random mask scheme of secret sharing. It can not only protect gradient privacy without losing model accuracy, but also resist equipment dropping and collusion attacks between devices, which has strong practicability. Secondly, we design an algorithm based on digital signature and hash function, which can not only achieve the integrity and consistency of the message, but also resist replay attacks. Finally, we use MNIST and CIFAR 10 data sets to prove that our scheme is safe in practice.

Key words edge calculation; edge gateway; federated learning; privacy protection

随着互联网和物联网的高速发展，手机、平板和电脑成了人们日常生活中必不可少的边缘智能计算设备[1]。通常，边缘智能计算场景包括智能医疗、智能家居、智能交通、智能教育等。边缘

收稿日期：2022－06－13；修回日期：2022－10－19
基金项目：国家自然科学基金 (62271128)；四川省科技计划重点研发项目 (2022ZDZX0004，23ZDYF0706，23ZDYF0085，2022YFG0212，2021YFS0391，2021YFG0027，2020YFG0475，2019YJ0543)；
作者简介：刘东 (1974－)，男，高级工程师，主要从事边缘计算和资源调度方面的研究.
*通信作者：王瑞锦，E-mail： wrj8882003@163.com

计算从云端计算延伸，在边缘部署地理分布的边缘网关网络，提供更接近物联网设备的计算能力。在传统的云端计算模式下，边缘智能终端直接将本地模型发送到云端进行计算处理，机器学习的集中训练模式可能会带来一些安全隐患，这种模式容易被攻击者拦截并发起隐私攻击[1-2]。此外，由于分布式用户数据具有多源特性、异质性等特点，集中处理会带来很大的资源开销和安全风险。边缘智能计算通过扩展边缘云端对中心云端进行补充，使得网络边缘能够满足计算和存储此类应用的要求[3]。

联邦学习是一种新型的分布式框架，与传统的集中式机器学习相比，具有更好的隐私保护功能。它的原理是组合多个分布式设备，保护本地各种设备协调下的数据集，共享局部模型参数，可以获得更准确的机器学习模型来自训练和学习，从而实现数据的“可用隐身”。

1 相关工作

联邦学习[4]是谷歌在 2016 年首次提出的分布式机器学习模式，目的是为了解决数据交换过程中存在的隐私泄露问题。传统的联邦学习系统是服务器和客户端模式，分为横向联邦学习、纵向联邦学习和联邦迁移学习，其中联邦迁移学习不对数据进行切分，利用迁移学习来克服标签不足的情况[5]。对比传统的机器学习，服务器将模型参数分配给不同的客户端，客户端只上传模型参数而不上传原始数据，从而可以将数据保存在本地，从一定程度上保护了用户隐私。

在现阶段的研究中，融合边缘智能计算和联邦学习的方案具有边缘化、分布式、资源动态性等特征，同时使隐私保护和合作共享成为可能。但是由于隐私攻击模型的出现，如梯度泄露攻击、重放攻击，使得模型的隐私性受到威胁。文献 [6] 指出，在智能家居中传感器与大量的用户隐私相关联，在数据的产生、传输、处理过程中都存在着隐私泄露的风险。文献 [7] 指出，车联网的部署在提供定位服务的同时也存在隐私泄露的风险。文献 [8] 通过将释放出的 Netflix 数据集与 IMDb 数据集进行关联就挖掘出了一部分用户的敏感信息，随后在推荐中对于数据的隐私保护方法进行了大量尝试，如匿名化、差分隐私、本地化的差分隐私、同态加密算法、安全多方计算等与推荐方法的结合；以及机器学习思想在推荐中的尝试，如对抗机器学习、对抗样本生成等，都在一定程度上保护了用户的隐私和安全。文献 [8] 设计了一个安全聚合方案，在聚合期间使用户能够更新加权向量平均，消除用户间的致盲因子。文献 [9] 基于协同学习设计了 GAN 攻击，使恶意用户加入训练过程并生成诚实的数据集用户。文献 [10] 添加拉普拉斯噪声到神经网络中的梯度以满足差分隐私。尽管如此，文献 [11] 指出虽然添加梯度噪声可以保证隐私，但它的签名大大降低了模型的准确性。文献 [12] 提出了一种基于加法同态加密的协同学习系统。

2 问题定义

设 D 和 D'是相邻数据集，即只有一个样本不同。对于查询函数 f，如果满足式 (1)，则 f 满足差分隐私：

$$\Pr[f(D)\in R]\leqslant e^{\varepsilon}\Pr[f(D)\in R]+\delta \tag{1}$$

式中，ε代表隐私度，ε越大代表数据可用性越高，越小代表隐私保护程度越高，相应地，添加的噪声越大，当ε为 0 时，代表没有添加差分隐私；δ代表置信度参数，在严格差分隐私中，δ为 0，当$\delta>0$时，为近似差分隐私，在实际工业中，近似差分隐私被广泛使用。

高斯机制：给定一个数据集 D 和查询函数 f，则提供差分隐私的机制 M 满足：

$$M(D)=f(D)+N(o,\sigma^2)$$

式中，σ代表标准差，需满足：

$$\sigma>\frac{\sqrt{2\ln(1.25/\delta)}\Delta f}{\varepsilon}$$

式中，Δf是数据集的敏感度；为相邻数据集的二范数。

设 u 和 v 分别为不同边缘网关的 ID 号，则其密钥为$S_(u,v)=\mathrm{KA.agree}(\mathrm{sSK},\mathrm{sPK})$，同维展开向量为$\boldsymbol{P}_{u,v}=\Delta_{u,v}*\mathrm{PNG}(S_{u,v})(u>v,\Delta_{u,v}=1;u<v,\Delta_{u,v}=-1)$

假设Δ_{ansg}是联邦聚合梯度， U 为边网关集，Δ_{yu}为边缘网关上传的参数，聚合规则如下：

$$\Delta_{\mathrm{ansg}}=\sum_{u\in U}\mathrm{yu}=\sum_{u}\left(\Delta_{\mathrm{yu}}+\sum_{u\in u:u<v}\mathrm{PRG}(S_{S,v})-\sum_{u\in u:u>v}\mathrm{PRG}(S_{S,v})\right)=\sum_{u\in U}\Delta_{\mathrm{yu}}$$

假设在第 t 轮训练，之前 r 个边缘网关得到的共享模型训练为 θ_t，并且在 θ_t上进行τ次迭代。$\theta_{t,s}$是第 t 轮训练、第 s 次迭代时边缘网关的本地模型。在每次迭代$s=0,1,\cdots,\theta-1$时，边缘网关通过以下规则更新其模型：$\theta_{(t,s+1)}=\theta_{(t,s)}-\eta g(\theta(t,s))$，其中 $g(\theta(t,s))=\frac{1}{B}\sum_{\xi\in X_i}\nabla l(\theta_i^{t,s},\xi)$表示基于从本地聚合数据集 D_i 中采样的 B 个样本点 X_i计算的随机梯度。

在第 t 轮训练中，共享模型的更新规则为：

$$\theta=\frac{1}{r}\sum\theta,\ \theta^{t+1}=\frac{1}{r}\sum_{i\in\Omega_t}\theta_i^{t,\tau}$$

在第 t 轮训练中，传输的数据量为 L，信道带宽为 B，因此传输时间为$m_t=L/B$。设 P 为第 t 轮训练的功率，那么产生的能量消耗为LP/B。

表 1 描述了本文方案相关算法。

表 1　相关算法描述表

算法	含义
KA.param()	公共参数生成
KA.gen()	公私钥对生成算法
KA.agree()	私有共享密钥生成算法
SS.share()	秘密分享算法
SS.recon()	秘密重建算法
SIG.gen()	密钥生成算法
SIG.sign()	签名算法
SIG.ver()	验证算法

3　方案设计

3.1　系统架构

为了解决边缘计算场景下训练全局机器学习模型的隐私泄露问题，设计了一种使用安全多方计算框架的联邦学习系统。该系统包括一个云端和多个可以与之通信的边缘网关，且边缘网关和边缘智能终端可以相互通信。图 1 为该系统架构，系统中有 3 种实体。

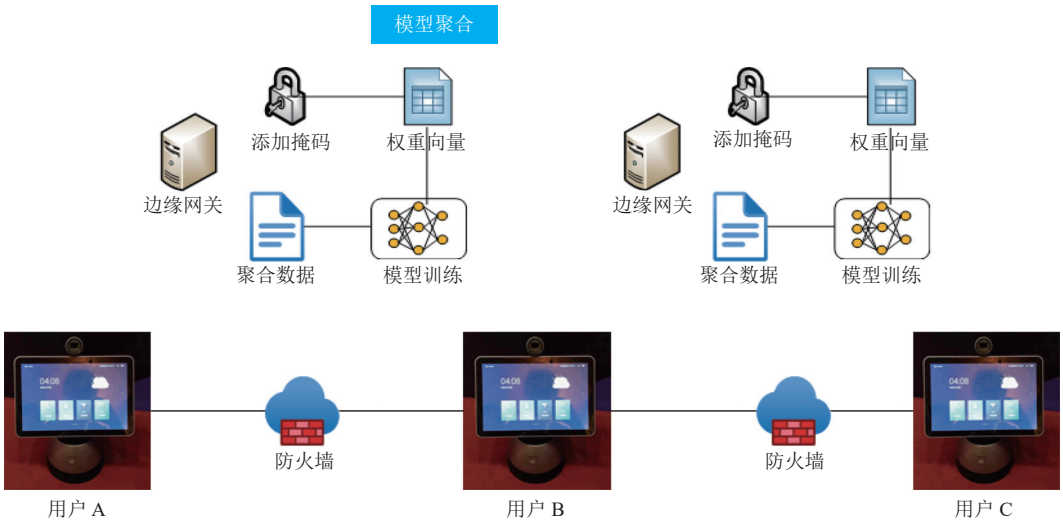

图 1　系统架构

1) 边缘智能终端：作为联邦学习任务的参与者，有不同数量的数据集和不同的计算能力，它们的加密数据集旨在训练一个模型。

2) 边缘网关：是边缘智能终端和云端的链接，具有更强的计算能力和更大的存储空间。它们从边缘智能终端收集加密数据并训练模型，并将训练好的模型参数发送到云端进行聚合。

3) 云端：是本文方案中的参数服务器。负责分发初始训练模型、聚合和更新模型参数。

首先，边缘智能终端使用不同的本地数据隐私保护，然后上传到边缘网关进行数据聚合，边缘网关数据聚合后，对本地模型进行训练，并对模型进行 PPCEF，然后上传到云端进行模型聚合，云端将模型聚合后，再下放到各边缘网关进行更新。

本文设计的 PPCEF 方案，首先使用基于 DH 密钥交换协议的 KA.agree() 函数使每个边缘网关使用私钥sSK与其他边缘网关公钥sPK来协商一个密钥$S_{u,v}$，使用该密钥作为随机数生成器种子PNG($S_{u,v}$)生成与模型梯度向量维数相同的扩展掩码$\boldsymbol{p}_{u,v}=\sum\Delta_{u,v}*\mathrm{PNG}(S_{u,v})$(其中，$u$ 表示该网关 ID，v 表示其他所有网关 ID)，并且要求当 $u>v$ 时，$\Delta_{u,v}=1$；当 $u<v$ 时，$\Delta_{u,v}=-1$。同时，每个边缘网关使用秘密共享方案SS.share(sSK)，并将每个秘密共享份额分发给其他边缘网关。以上过程就是添加个人掩

码。为了防止云端直接获得聚合结果，每个边缘网关都需要使用 PNG 生成一个随机数b_u，并将其扩展为相同维度的向量$\boldsymbol{p}_{u,\text{prav}}$，并分配到每个边缘网关。每个边缘网关计算$\boldsymbol{p}_{\text{pub}}=\sum \boldsymbol{p}_{u,\text{prav}}$作为边缘网关的公共掩码。

其次，如果每个边缘网关都参与训练，因为密钥交换协议使边缘网关 u、v 协商了相同的$S_{u,v}$，且$\Delta_{u,v}*\text{PNG}(S_{u,v})$。 当 $u>v$ 时，$\Delta_{u,v}=1$； 当 $u<v$ 时，$\Delta_{u,v}=-1$。因此，云端聚合中所有个人掩码的总和为 $\boldsymbol{0}$ 向量；同时，云端可以收集掉线的边缘网关分发给其他边缘网关的私钥的秘密份额进行秘密重构$\text{SS.recon}\left(\left\{S_{u,v}^{\text{SK}}\right\}v\in U\right)$ (其中 U 为在线网关集合； u 代表离线网关)，恢复S_u^{SK}，云端通过S_u^{SK}、公开的公钥信息 PNG 和重构出掉线网关的$\boldsymbol{p}_{u,v}$，这样个人掩码加和为 $\boldsymbol{0}$ 向量。 云端使用联邦平均算法完成全局梯度向量的聚合时，不用考虑个人掩码向量与 $\boldsymbol{0}$ 向量之和，返回给边缘网关的计算结果只需要减去公共掩码向量$\boldsymbol{p}_{\text{pub}}$就能得到全局梯度平均值。

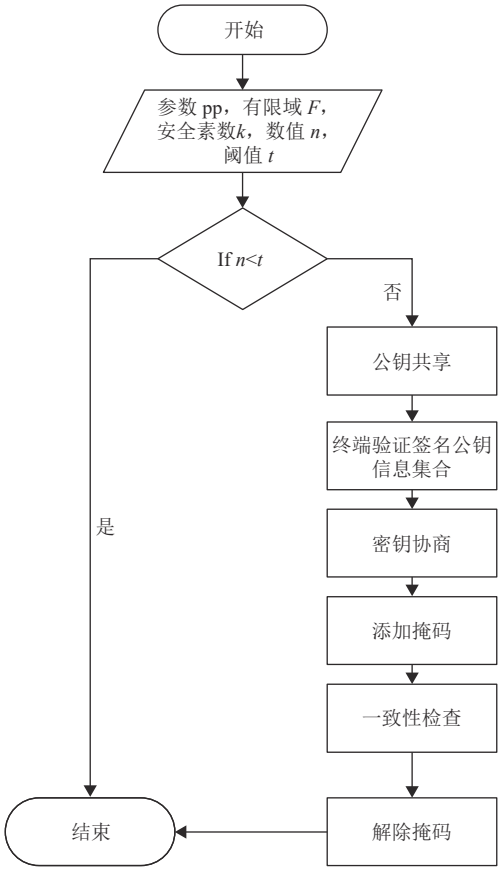

图 2 PPCEF 隐私保护算法流程图

最后，由于个人掩码的存在，联邦学习的每个参与者无法知道单个边缘网关上传的本地模型梯度，这保证了每个边缘网关的隐私。 由于秘密共享算法的存在，恶意用户都不能通过共谋攻击来攻击系统中的参与者。 这种安全性在理论上是有保证的，同时边缘网关也有一定的冗余性。 因为公共掩码的存在，全局模型梯度在传输过程中不暴露，保证了全局模型梯度的安全性。其算法流程如图 2 所示。

3.2 初始化

在进行联合学习之前，系统需要设置一些必要的参数，以保证系统传输和安全的需要。

1) 生成云端边缘网关和云端公钥证书，进行身份认证，实现公钥与身份的唯一绑定关系。系统主要使用公钥和私钥对(dSK,dPK)进行身份认证和消息认证。

2) 从云端生成一个安全质数 k，k 的位数必须大于 1 024。

3) 为秘密共享算法指定一个有限字段 F。

4) 在各边缘终端与边缘网关、边缘网关与云端之间建立相应的通信路径。在实验中使用一个相对简单的 socket 机制来实现每个参与者之间的通信互连。

5) 设置秘密共享协议的参数 n 和 t。

6) 所有参与训练的边缘网关都诚实地使用云端提供的安全质数 k，来生成与 DH 密钥交换协议相关的参数$\text{pp}\leftarrow\text{KA.param}(k)$。

3.3 公共密钥共享

1) 边缘智能终端对原始数据 d 添加差分隐私保护机制，$M(d)=f(d)+N(o,\sigma^2)$，其中 N 是高斯分布，σ 是 d 的方差。然后将处理后的数据发送到附近的边缘网关进行多用户数据聚合。

2) 训练好的边缘网关使用公钥生成算法生成两个公私钥对$(c_u^{\text{PK}},c_u^{\text{SK}})\leftarrow\text{KA.gen(pp)}$和$(s_u^{\text{pk}},s_u^{\text{SK}})\leftarrow\text{KA.gen(pp)}$，并使用个人签名私钥对公钥进行签名$\sigma_u\leftarrow\text{SIG.sign}(d_u^{\text{SK}},c_u^{\text{PK}}\|s_u^{\text{PK}})$。每个边缘网关拼接后得$c_u^{\text{PK}}\|s_u^{\text{PK}}\|\sigma_u\|\text{timestamp}$并经过 base64 编码后通过 socket 连接到云端。

3) 云端收集参与训练的边缘网关发送的信息，当收集一定时间且记录的参与训练的边缘网关数量未达到 t 及以上时，聚合训练将被中断。 否则，云端广播训练网关集合 $U1$ 和签名公钥信息。

3.4 密钥协商

1) 参加训练的边缘网关收到终端集 $U1$ 和云端广播的签名公钥信息集后检查时间戳；验证

$\forall v \in U1, \mathrm{SIG.ver}(d_v^{\mathrm{PK}}, c_v^{\mathrm{PK}} \| s_v^{\mathrm{PK}}, \sigma u) = 1$，如果验证通过，则生成秘密共享；否则，训练中断。

2) 参与训练的边缘网关使用随机数生成器 PRG 生成两个属于有限域 F 的随机数b_u。

3) 边缘网关生成一个秘密多项式：

$$F(x) = Bu + a_1 x + a_2 x2 + \cdots$$

4) 使用秘密共享算法生成秘密共享：$(v, s_{u,v}^{\mathrm{SK}})_{v \in U1} \leftarrow \mathrm{SS.share}(s_u^{\mathrm{SK}}, t, U1)$。

5) 边缘网关对于每个其他边缘网关 $v \in U1$，加密得到：$e_{u,v} \leftarrow \mathrm{AE.enc}(\mathrm{KA.agree}(c_u^{\mathrm{SK}}, c_v^{\mathrm{PK}}), u \| v \| b_u \| s_{u,v}^{\mathrm{SK}})$。

6) 边缘网关使用 SHA128 算法取消息摘要并使用签名公钥d_u^{PK}进行签名$\theta_{u,v} \leftarrow \mathrm{SIG.sign}(d_u^{\mathrm{SK}}, \mathrm{Hash}(e_{u,v}))$。

7) 边缘网关发送消息$(e_{u,v} \| \mathrm{Hash}(e_{u,v}) \| \theta_{u,v} \| \mathrm{timestamp})$通过 socket 发送到云端。

8) 从云端采集至少 T 条密文信息，参与训练的边缘网关记为 $U2$。检查 $U2 \subseteq U1$，如果不能证明，则终止，否则继续进行掩码添加。

9) 云端广播签名秘密消息$(e_{u,v} \| \mathrm{Hash}(e_{u,v}) \| \theta_{u,v} \| \mathrm{timestamp})$和边缘网关的集合 $U2$。

3.5　掩码添加

1) 参与的边缘网关接收签名秘密来自云端的信息并将其保存为列表。

2) 边缘网关以每个网关的随机数b_u作为种子，用 PRG 扩展为随机向量$\boldsymbol{p}_{u,\mathrm{prav}}(u \in U2)$，计算公共掩码向量$\boldsymbol{p}_{\mathrm{pub}} = \sum \boldsymbol{p}_{u,\mathrm{prav}}$。

3) 计算掩码梯度向量$\boldsymbol{y}_u \leftarrow \boldsymbol{x}_u + \boldsymbol{p}_{\mathrm{pub}} + + \sum_{v \in U2} \boldsymbol{p}_{u,v} (\mathrm{mod} R)$，并添加到掩码。

4) 对掩码梯度向量进行压缩并使用签名公钥进行签名，$\boldsymbol{\gamma}_{u,v} \leftarrow \mathrm{SIG.sign}(d_u^{\mathrm{SK}}, \boldsymbol{y}_u)$

5) 将 $(\boldsymbol{y}_u \| \boldsymbol{\gamma}_{u,v} \| \mathrm{timestamp})$发送到云端，等待云端反馈。

6) 云端接受至少 t 条签名掩码权重向量信息，并记录这些边缘网关为集合 $U3$。检查 $U3 \subseteq U2$，如果不成立，则终止，否则广播签名掩码梯度向量信息$(\boldsymbol{y}_u \| \boldsymbol{\gamma}_{u,v} \| \mathrm{timestamp})$和边缘网关集 $U3$。

3.6　一致性检查

1) 边缘网关从云端接收边缘网关集 $U3$，$\subseteq$如果 $U3<t$，则中止。

2) 边缘网关将 $\mu_u \leftarrow (U3 \| \mathrm{SIG.sign}(d_u^{\mathrm{SK}}, U3 \| \mathrm{timestamp}))$发送到云端。

3) 云端从至少 t 个边缘网关处收集μ_u(用$U4 \subseteq U3$表示这组用户)，向 $U4$ 中的每个边缘网关发送集$\{v, \mu_u\}_{v \in U4}$。

3.7　解除掩码

1) 从云端接收合$\{v, \mu_u\}_{v \in U4}$，验证$U4 \subseteq U3, U4 > t$ 和消息的新鲜性，根据每个边缘网关签名验证公钥来验证$\mathrm{SIG.ver}(d^{\mathrm{PK}}, U3, \mu_u)$是否等于 1。

2) 向云端发送掉线边缘网关秘密份额$s_{u,v}^{\mathrm{SK}}(v \in U2 \backslash U3)$。

3) 参与训练的边缘网关收到云端发来的消息，并进行签名验证。

4) 边缘网关计算联合聚合梯度 $\mathrm{ans} = \boldsymbol{z} - \boldsymbol{p}_{\mathrm{pub}}$并将其加载到本地模型中，为下一轮联合训练做准备。当训练取得良好效果时，向边缘终端提供服务反馈。

5) 从至少 t 个边缘网关收集响应并将这些边缘网关记录在 $U5$ 中。

6) 对于 $U \in U2$ 中的每个网关，重构$S_u^{\mathrm{SK}} \leftarrow \mathrm{SS.recon}(\{s_{u,v \in U5}^{\mathrm{SK}}, t\})$并使用它 (连同在 AdvertiseKeys 接收的公钥) 重新计算所有$v \subseteq U3$的$\boldsymbol{p}_{u,v}$。

7) 对于每个网关 $U \in U3$，重构 $b_u \leftarrow \mathrm{SS.recon}(\{\boldsymbol{b}_{u,v \in U5}\}, t)$，然后使用 PRG 重新计算$\boldsymbol{p}_u$。

8) 云端使用签名公钥进行广播压缩向量签名。

4　实验分析

4.1　实验配置

本实验采用 MNIST[13-14] 数据集和 CIFAR10[15] 数据集进行对比分析。将原有的联邦学习算法作为比较基准，并将基于主流隐私保护方案的联邦学习验证隐私方法与 PPCEF 进行比较，以实现对比分析。

4.2　实验对比分析

4.2.1　精度

3 种方案在 MNIST 数据集上进行训练，得到图 3 所示的 ACC(精度) 曲线。可以看出，使用 MNIST[12] 数据集进行 16 轮训练后，本文的 PPCEF 模型准确率达到 90%。在使用 CIFAR10 数据集时，从图 4 可以看到，经过 30 轮训练，PPCEF 模型的准确率达到了 95%，它更接近于原始的联合学习，但明显高于差异隐私方案。

可以看出，原始的联邦学习方案精度略高于 PPCEF，但原始联邦学习没有添加隐私保护方案，存在隐私风险，而面对一个不安全的网络环境，隐私保护方案是必不可少的。

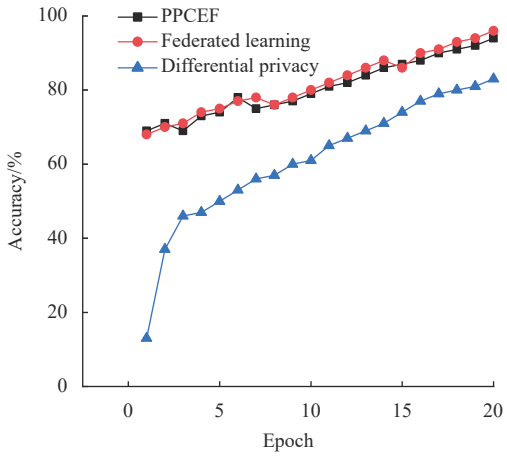

图 3　3 种方案的精度比较 (MNIST)

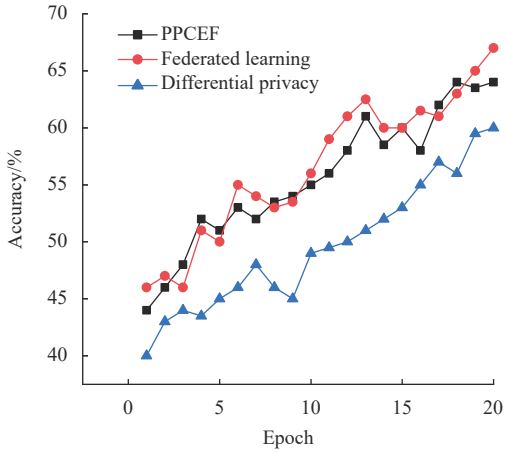

图 4　3 种方案的精度比较 (CIFAR10)

4.2.2　防隐私攻击能力

学习系统使用该安全方案，由于梯度添加掩码，使得即使在迭代后，虚拟梯度最大程度接近“真实梯度”，但“真实梯度”是添加掩码的虚假梯度，所以无论迭代多少次，攻击者只有无用的虚假梯度，因此，原始图像不能从梯度恢复。使用梯度泄漏攻击[14]来测试 PPCEF 的反隐私攻击能力，并将 PPCEF 攻击结果与原始联邦学习攻击结果进行比较。当原始联邦学习迭代次数为 130 时，原始图像基本恢复。但是，由于 PPCEF 在梯度上添加了掩码，原始图像不会暴露。

4.2.3　边缘网关能耗对比分析

分析了 FedAvg[15]、q-FedSGD[16] 和 PPCEF 中各边缘网关参与联邦学习的总能量消耗，能量消耗描述了参与联邦学习的成本。

表 2 给出了 3 种算法中每个边缘网关学习的总能耗。3 种算法下各边缘网关的能耗分布趋势和时间分布是相似的。

表 2　能耗比较

s

The gateway Numbers	FedAvg[4]	q-FedSGD[10]	PPCEF
0	1×10 000	2×1 000	2×100
1	2×10 000	1×10 000	3×1 000
2	1×100 000	1.5×10 000	1×1 000
3	1.5×10 000	1.5×1 000	8×100
4	1×10 000	1×1 000	1×10 000
5	1×1 000	5×100	1×100

5　结 束 语

在当前的边缘计算网络中，隐私安全问题尤为突出。因此，如何将传统的隐私保护方案与边缘计算环境中的边缘数据处理特征相结合，从而实现多元化服务环境下的用户隐私保护就显得尤为重要。

本文以边缘计算为研究对象，介绍了联邦学习的训练框架，设计了一种基于秘密共享和权重掩码的轻量级隐私保护协议，能够很好地达到隐私保护的目的。

参 考 文 献

[1] XU G, LI H, REN H, et al. Data security issues in deep learning: Attacks, countermeasures, and opportunities[J]. IEEE Communications Magazine: Articles, News, and Events of Interest to Communications Engineers, 2019, 57(11): 116-122.

[2] KIM T, JUNG I Y, HU Y C. Automatic, location-privacy preserving dashcam video sharing using blockchain and deep learning[J]. Human-centric Computing and Information Sciences, 2020, 10(11): 1-23.

[3] SANTOS J, WAUTERS T, VOLCKAERT B, et al. Fog computing: Enabling the management and orchestration of smart city applications in 5G networks[J]. Entropy, 2018, 20(15): 138-144.

[4] LU Y, HUANG X, ZHANG K, et al. Communication-efficient federated learning for digital twin edge networks in industrial IOT[J]. IEEE Transactions on Industrial Informatics, 2021, 17(13): 5709-5718.

[5] MA X, ZHANG F, CHEN X, et al. Privacy preserving multi-party computation delegation for deep learning in cloud computing[J]. Information Sciences: An International Journal, 2018, 459(17): 103-116.

[6] KUANG B Y, FU A M, YU S, et al. ESDRA: An efficient and secure distributed remote attestation scheme for IoT swarms[J]. IEEE Internet of Things Journal, 2019, 6(8): 8372-8383.

[7] LAURA D A, BROMBERG F, DUJOVNE D, et al. Prediction of frost events using machine learning and IOT sensing devices[J]. IEEE Internet of Things Journal, 2018, 5(6): 4589-4597.

[8] WANG B, LI M, CHOW S S M, et al. Computing

encrypted cloud data efficiently under multiple keys[C]//2013 IEEE Conference on Communications and Network Security (CNS). [S. l.]: IEEE, 2013, 12: 504-513.

[9] ZHAO L, WANG Q, ZOU Q, et al. Privacy-preserving collaborative deep learning with unreliable participants[J]. IEEE Transactions on Information Forensics and Security, 2020, 15(12): 1486-1500.

[10] ZHANG J, ZHAO Y, WANG J, et al. Fedmec: Improving efficiencyof differentially private federated learning via mobile edge computing[J]. Mobile Networks and Applications, 2020, 10(9): 1-13.

[11] ZHANG J, CHEN X, XU G, et al. Universal quantum circuit evaluation on encrypted data using probabilistic quantum homomorphic encryption scheme[J]. Chinese Physics B, 2021, 16(15): 1204-1209.

[12] SCHOTT L, RAUBER J, BETHGE M, et al. Towards the first adversarially robust neural network model on mnist[EB/OL]. [2021-05-11]. https://arxiv.org/pdf/1805.09190.pdf.

[13] LI H M, LIU H C, JI X Y, et al. CIFAR10-DVS: An event-stream dataset for object classification[J]. Frontiers in Neuroscience, 2017, 11(10): 847-858.

[14] DENG J, WANG Y, LI J, et al. TAG: Gradient attack on transformer-based language models[EB/OL]. [2022-05-16]. https://www.xueshufan.com/publication/3199487019.

[15] ZHOU Y, YE Q, LV J, et al. Communication-Efficient federated learning with compensated overlap-FedAvg[J]. IEEE Transactions on Parallel and Distributed Systems, 2022, 33(12): 192-205.

[16] MEERZA S I A, LI Z H, LIU L Y, et al. Fair and privacy-preserving Alzheimer's disease diagnosis based on spontaneous speech analysis via federated learning[C]//2022 44th Annual International Conference of the IEEE Engineering in Medicine & Biology Society (EMBC). [S. l.]: IEEE, 2022, 44: 1362-1365.

编　辑　叶　芳