(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 109492420 B
(45)授权公告日 2021.07.20

(21)申请号 201811620130.X

(22)申请日 2018.12.28

(65)同一申请的已公布的文献号
申请公布号 CN 109492420 A

(43)申请公布日 2019.03.19

(73)专利权人 深圳前海微众银行股份有限公司
地址 518052 广东省深圳市前海深港合作区前湾一路1号A栋201室(入驻深圳市前海商务秘书有限公司)

(72)发明人 刘洋 康焱 陈天健 杨强 范涛

(74)专利代理机构 深圳市世纪恒程知识产权代理事务所 44287
代理人 胡海国

(51)Int.Cl.
G06F 21/60(2013.01)
G06K 9/62(2006.01)

(56)对比文件
CN 109002861 A,2018.12.14
CN 109034398 A,2018.12.18
CN 108764159 A,2018.11.06
CN 106096641 A,2016.11.09
US 2008103996 A1,2008.05.01
CN 106649434 A,2017.05.10
CN 108305167 A,2018.07.20
US 2008082475 A1,2008.04.03

审查员 赵玉华

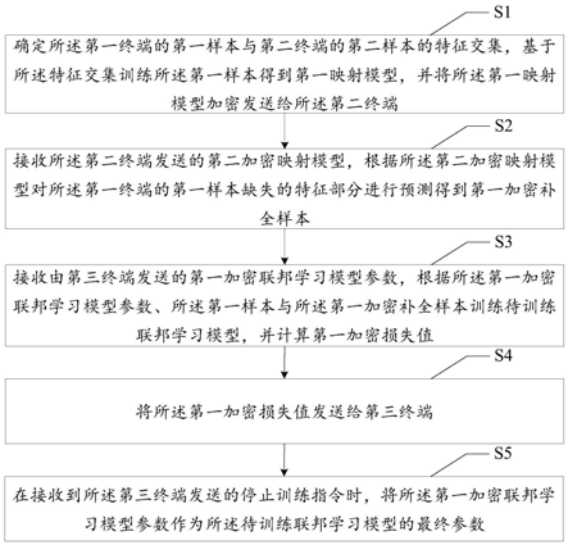
权利要求书3页 说明书16页 附图3页

(54)发明名称

基于联邦学习的模型参数训练方法、终端、系统及介质

(57)摘要

本发明公开了一种基于联邦学习的模型参数训练方法、终端、系统及介质，该方法包括：确定第一终端的第一样本与第二终端的第二样本的特征交集，基于特征交集训练第一样本得到第一映射模型，并发送给第二终端；接收第二终端发送的第二加密映射模型，并对第一样本缺失的特征部分进行预测得到第一加密补全样本；接收由第三终端发送的第一加密联邦学习模型参数，根据第一加密联邦学习模型参数训练待训练联邦学习模型，并计算第一加密损失值；将第一加密损失值发送给第三终端；在接收到第三终端发送的停止训练指令时，则将第一加密联邦学习模型参数作为待训练联邦学习模型的最终参数。本发明实现了利用迁移学习对联邦双方特征空间进行拓展，提高联邦模型的预测能力。



CN 109492420 B

1.一种基于联邦学习的模型参数训练方法,其特征在于,所述基于联邦学习的模型参数训练方法应用于第一终端,所述基于联邦学习的模型参数训练方法包括以下步骤:

确定所述第一终端的第一样本与第二终端的第二样本的特征交集,基于所述特征交集训练所述第一样本得到第一映射模型,并将所述第一映射模型加密发送给所述第二终端,以供所述第二终端对所述第二样本缺失的特征部分进行预测得到第二加密补全样本;

接收所述第二终端发送的第二加密映射模型,根据所述第二加密映射模型对所述第一终端的第一样本缺失的特征部分进行预测得到第一加密补全样本,所述第二加密映射模型是所述第二终端基于所述特征交集训练所述第二样本得到;

接收由第三终端发送的第一加密联邦学习模型参数,根据所述第一加密联邦学习模型参数、所述第一样本与所述第一加密补全样本训练待训练联邦学习模型,并计算第一加密损失值;

将所述第一加密损失值发送给第三终端,以供所述第三终端根据所述第一加密损失值与第二加密损失值计算损失和,根据所述损失和判断所述待训练联邦学习模型是否处于收敛状态,所述第二加密损失值由所述第二终端根据所述第二样本、所述第二加密补全样本以及所述第三终端发送的所述第一加密联邦学习模型参数计算得到;

在接收到所述第三终端发送的停止训练指令时,将所述第一加密联邦学习模型参数作为所述待训练联邦学习模型的最终参数,所述停止训练指令由所述第三终端在判定所述待训练联邦学习模型处于收敛状态后发出。

2.如权利要求1所述的基于联邦学习的模型参数训练方法,其特征在于,所述在接收到所述第三终端发送的停止训练指令时,则将所述第一加密联邦学习模型参数作为所述待训练联邦学习模型的最终参数的步骤之后还包括:

基于所述待训练联邦学习模型的最终参数与所述第一样本或者所述第一加密补全样本计算得到第一加密预测结果,将所述第一加密预测结果发送给所述第三终端;

在所述第三终端对所述第一加密预测结果解密后,获取所述第三终端解密得到的第一预测结果。

3.如权利要求1所述的基于联邦学习的模型参数训练方法,其特征在于,所述将所述第一加密损失值发送给第三终端,以供所述第三终端根据所述第一加密损失值与第二加密损失值计算损失和,根据所述损失和判断所述待训练联邦学习模型是否处于收敛状态的步骤之后还包括:

在接收到所述第三终端发送的继续训练指令时,计算并将与所述第一加密损失值对应的第一加密梯度值发送给所述第三终端,以供所述第三终端根据所述第一加密梯度值与第二加密梯度值计算梯度和,根据所述梯度和更新所述第一加密联邦学习模型参数,得到第二加密联邦学习模型参数,所述第二加密梯度值由所述第二终端根据所述第二样本、所述第二加密补全样本以及所述第三终端发送的所述第一加密联邦学习模型参数计算得到,所述继续训练指令由所述第三终端在判定所述待训练联邦学习模型处于未收敛状态时发出;

获取由所述第三终端发送的所述第二加密联邦学习模型参数,并根据所述第二加密联邦学习模型参数计算所述第一终端的第三加密损失值;

将所述第三加密损失值发送给第三终端,以供所述第三终端根据所述第三加密损失值与第四加密损失值计算新的损失和,根据所述新的损失和判断所述待训练联邦学习模型是

否处于收敛状态，所述第四加密损失值由所述第二终端根据所述第二样本、所述第二加密补全样本以及所述第三终端发送的所述第二加密联邦学习模型参数计算得到；

在接收到所述第三终端发送的停止训练指令时，则将所述第二加密联邦学习模型参数作为所述待训练联邦学习模型的最终参数。

4.一种基于联邦学习的模型参数训练方法，其特征在于，所述基于联邦学习的模型参数训练方法应用于第三终端，所述基于联邦学习的模型参数训练方法包括以下步骤：

在第一终端利用第二终端的第二加密映射模型对所述第一终端的第一样本缺失的特征部分进行预测得到第一加密补全样本，所述第二终端利用所述第一终端的第一加密映射模型对所述第二终端的第二样本缺失的特征部分进行预测得到第二加密补全样本之后，所述第三终端向所述第一终端和所述第二终端发送第一加密联邦学习模型参数，以供所述第一终端根据所述第一加密联邦学习模型参数、所述第一样本与所述第一加密补全样本计算第一加密损失值，以及所述第二终端根据所述第一加密联邦学习模型参数、所述第二样本与所述第二加密补全样本计算第二加密损失值，其中，所述第二加密映射模型由所述第一样本与所述第二样本的特征交集训练所述第二样本得到，所述第一加密映射模型由所述特征交集训练所述第一样本得到；

接收并根据由所述第一终端发送的所述第一加密损失值与由所述第二终端发送的所述第二加密损失值计算损失和，并根据所述损失和判断待训练联邦学习模型是否处于收敛状态；

若所述待训练联邦学习模型处于收敛状态，则将所述第一加密联邦学习模型参数作为所述待训练联邦学习模型的最终参数。

5.如权利要求4所述的基于联邦学习的模型参数训练方法，其特征在于，所述若所述待训练联邦学习模型处于收敛状态，则将所述第一加密联邦学习模型参数作为所述待训练联邦学习模型的最终参数的步骤之后还包括：

接收到所述第一终端发送的第一加密预测结果；

解密所述第一加密预测结果得到第一预测结果，将解密得到的所述第一预测结果发送给所述第一终端。

6.如权利要求4所述的基于联邦学习的模型参数训练方法，其特征在于，所述接收并根据由所述第一终端发送的所述第一加密损失值与由所述第二终端发送的所述第二加密损失值计算损失和，并根据所述损失和判断所述待训练联邦学习模型是否处于收敛状态的步骤之后还包括：

若判定所述待训练联邦学习模型处于未收敛状态，则向所述第一终端和所述第二终端发送继续训练指令；

接收并根据所述第一终端发送的第一加密梯度值和所述第二终端发送的第二加密梯度值计算梯度和，根据所述梯度和更新所述第一加密联邦学习模型参数，得到第二加密联邦学习模型参数，将所述第二加密联邦学习模型参数发送给所述第一终端和所述第二终端；

接收并根据所述第一终端发送的第三加密损失值和所述第二终端发送的第四加密损失值计算新的损失和，并根据所述新的损失和判断所述待训练联邦学习模型是否处于收敛状态，所述第三加密损失值由所述第一终端根据所述第一样本、所述第一加密补全样本以

及所述第三终端发送的所述第二加密联邦学习模型参数计算得到，所述第四加密损失值由所述第二终端根据所述第二样本、所述第二加密补全样本以及所述第三终端发送的所述第二加密联邦学习模型参数计算得到；

若所述待训练联邦学习模型处于收敛状态，则向所述第一终端和所述第二终端发送停止训练指令，并将所述第二加密联邦学习模型参数作为所述待训练联邦学习模型的最终参数。

7.如权利要求4所述的基于联邦学习的模型参数训练方法，其特征在于，所述根据所述损失和判断所述待训练联邦学习模型是否处于收敛状态的步骤包括：

根据所述损失和是否小于或者等于预设阈值，判断所述待训练联邦学习模型是否处于收敛状态；

若所述损失和小于或者等于预设阈值，则判定所述待训练联邦学习模型处于收敛状态；

若所述损失和大于预设阈值，则判定所述待训练联邦学习模型处于未收敛状态。

8.一种终端，其特征在于，所述终端包括：存储器、处理器及存储在所述存储器上并可在所述处理器上运行的基于联邦学习的模型参数训练程序，所述基于联邦学习的模型参数训练程序被所述处理器执行时实现如权利要求1至3中任一项所述的基于联邦学习的模型参数训练方法的步骤。

9.一种终端，其特征在于，所述第三终端包括：存储器、处理器及存储在所述存储器上并可在所述处理器上运行的基于联邦学习的模型参数训练程序，所述基于联邦学习的模型参数训练程序被所述处理器执行时实现如权利要求4至7中任一项所述的基于联邦学习的模型参数训练方法的步骤。

10.一种基于联邦学习的模型参数训练系统，其特征在于，所述基于联邦学习的模型参数训练系统包括：至少一个第一终端、至少一个第三终端、至少一个能与所述第一终端和所述第三终端交互的第二终端，所述 第一终端为权利要求8所述的终端、所述第三终端为权利要求9所述的终端。

11.一种存储介质，其特征在于，应用于计算机，所述存储介质上存储有基于联邦学习的模型参数训练程序，所述基于联邦学习的模型参数训练程序被处理器执行时实现如权利要求1至7中任一项所述的基于联邦学习的模型参数训练方法的步骤。

基于联邦学习的模型参数训练方法、终端、系统及介质

技术领域

[0001] 本发明涉及数据处理技术领域，尤其涉及一种基于联邦学习的模型参数训练方法、终端、系统及介质。

背景技术

[0002] 在人工智能领域，传统的数据处理模式往往是一方收集数据，再转移到另一方进行处理、清洗并建模，最后把模型卖给第三方。但随着法规完善和监控愈加严格，如果数据离开收集方或者用户不清楚模型的具体用途，运营者都可能会触犯法律。数据是以孤岛的形式存在的，解决孤岛的直接方案就是把数据整合到一方进行处理。但是，现在这样做很可能是违法的，因为法律不允许运营者粗暴地进行数据聚合。

[0003] 为解决此困境，人们研究提出了“联邦学习”的概念。联邦学习利用技术算法加密建造的模型，联邦双方在不用给出己方数据的情况下，也可进行模型训练得到模型参数，联邦学习通过加密机制下的参数交换方式保护用户数据隐私，数据和模型本身不会进行传输，也不能反猜对方数据，因此在数据层面不存在泄露的可能，也不违反更严格的数据保护法案如GDPR(General Data Protection Regulation,《通用数据保护条例》)等，能够在较高程度保持数据完整性的同时，保障数据隐私。

[0004] 但目前现有的横向联邦方法只能应用在联邦双方A、B样本均有标注，且双方的特征维度相同的情况，而对于A、B双方特征维度不同的情况不适用。因此，如何在保证两方的数据隐私与模型不被泄露的约束下，对A、B双方的特征空间进行拓展，进而提高联邦模型的预测能力，是亟待解决的问题。

发明内容

[0005] 本发明的主要目的在于提供一种基于联邦学习的模型参数训练方法、终端、系统及介质，旨在基于联邦双方样本的特征空间不同的情况下，实现在保证两方的数据隐私与模型不被泄露的约束下，利用迁移学习对联邦双方特征空间进行拓展，进而提高联邦模型的预测能力。

[0006] 为实现上述目的，本发明提供一种基于联邦学习的模型参数训练方法，所述基于联邦学习的模型参数训练方法应用于第一终端，所述基于联邦学习的模型参数训练方法包括以下步骤：

[0007] 确定所述第一终端的第一样本与第二终端的第二样本的特征交集，基于所述特征交集训练所述第一样本得到第一映射模型，并将所述第一映射模型加密发送给所述第二终端，以供所述第二终端对所述第二样本缺失的特征部分进行预测得到第二加密补全样本；

[0008] 接收所述第二终端发送的第二加密映射模型，根据所述第二加密映射模型对所述第一终端的第一样本缺失的特征部分进行预测得到第一加密补全样本，所述第二加密映射模型是所述第二终端基于所述特征交集训练所述第二样本得到；

[0009] 接收由第三终端发送的第一加密联邦学习模型参数，根据所述第一加密联邦学习

模型参数、所述第一样本与所述第一加密补全样本训练待训练联邦学习模型，并计算第一加密损失值；

[0010] 将所述第一加密损失值发送给第三终端，以供所述第三终端根据所述第一加密损失值与第二加密损失值计算损失和，根据所述损失和判断所述待训练联邦学习模型是否处于收敛状态，所述第二加密损失值由所述第二终端根据所述第二样本、所述第二加密补全样本以及所述第三终端发送的所述第一加密联邦学习模型参数计算得到；

[0011] 在接收到所述第三终端发送的停止训练指令时，则将所述第一加密联邦学习模型参数作为所述待训练联邦学习模型的最终参数，所述停止训练指令由所述第三终端在判定所述待训练联邦学习模型处于收敛状态后发出。

[0012] 可选地，所述在接收到所述第三终端发送的停止训练指令时，则将所述第一加密联邦学习模型参数作为所述待训练联邦学习模型的最终参数的步骤之后还包括：

[0013] 基于所述待训练联邦学习模型的最终参数与所述第一样本或者所述第一加密补全样本计算得到第一加密预测结果，将所述第一加密预测结果发送给所述第三终端；

[0014] 在所述第三终端对所述第一加密预测结果解密后，获取所述第三终端解密得到的第一预测结果。

[0015] 可选地，所述将所述第一加密损失值发送给第三终端，以供所述第三终端根据所述第一加密损失值与第二加密损失值计算损失和，根据所述损失和判断所述待训练联邦学习模型是否处于收敛状态的步骤之后还包括：

[0016] 在接收到所述第三终端发送的继续训练指令时，计算并将与所述第一加密损失值对应的第一加密梯度值发送给所述第三终端，以供所述第三终端根据所述第一加密梯度值与第二加密梯度值计算梯度和，根据所述梯度和更新所述第一加密联邦学习模型参数，得到第二加密联邦学习模型参数，所述第二加密梯度值由所述第二终端根据所述第二样本、所述第二加密补全样本以及所述第三终端发送的所述第一加密联邦学习模型参数计算得到，所述继续训练指令由所述第三终端在判定所述待训练联邦学习模型处于未收敛状态时发出；

[0017] 获取由所述第三终端发送的所述第二加密联邦学习模型参数，并根据所述第二加密联邦学习模型参数计算所述第一终端的第三加密损失值；

[0018] 将所述第三加密损失值发送给第三终端，以供所述第三终端根据所述第三加密损失值与第四加密损失值计算新的损失和，根据所述新的损失和判断所述待训练联邦学习模型是否处于收敛状态，所述第四加密损失值由所述第二终端根据所述第二样本、所述第二加密补全样本以及所述第三终端发送的所述第二加密联邦学习模型参数计算得到；

[0019] 在接收到所述第三终端发送的停止训练指令时，则将所述第二加密联邦学习模型参数作为所述待训练联邦学习模型的最终参数。

[0020] 本发明提供一种基于联邦学习的模型参数训练方法，所述基于联邦学习的模型参数训练方法应用于第三终端，所述基于联邦学习的模型参数训练方法包括以下步骤：

[0021] 在第一终端利用第二终端的第二加密映射模型对所述第一终端的第一样本缺失的特征部分进行预测得到第一加密补全样本，所述第二终端利用所述第一终端的第一加密映射模型对所述第二终端的第二样本缺失的特征部分进行预测得到第二加密补全样本之后，所述第三终端向所述第一终端和所述第二终端发送第一加密联邦学习模型参数，以供

所述第一终端根据所述第一加密联邦学习模型参数、所述第一样本与所述第一加密补全样本计算第一加密损失值，以及所述第二终端根据所述第一加密联邦学习模型参数、所述第二样本与所述第二加密补全样本计算第二加密损失值，其中，所述第二加密映射模型由所述第一样本与所述第二样本的特征交集训练所述第二样本得到，所述第一加密映射模型由所述特征交集训练所述第一样本得到；

[0022] 接收并根据由所述第一终端发送的所述第一加密损失值与由所述第二终端发送的所述第二加密损失值计算损失和，并根据所述损失和判断所述待训练联邦学习模型是否处于收敛状态；

[0023] 若所述待训练联邦学习模型处于收敛状态，则将所述第一加密联邦学习模型参数作为所述待训练联邦学习模型的最终参数。

[0024] 可选地，所述若所述待训练联邦学习模型处于收敛状态，则将所述第一加密联邦学习模型参数作为所述待训练联邦学习模型的最终参数的步骤之后还包括：

[0025] 接收到所述第一终端发送的第一加密预测结果；

[0026] 解密所述第一加密预测结果得到第一预测结果，将解密得到的所述第一预测结果发送给所述第一终端。

[0027] 可选地，所述接收并根据由所述第一终端发送的所述第一加密损失值与由所述第二终端发送的所述第二加密损失值计算损失和，并根据所述损失和判断所述待训练联邦学习模型是否处于收敛状态的步骤之后还包括：

[0028] 若判定所述待训练联邦学习模型处于未收敛状态，则向所述第一终端和所述第二终端发送继续训练指令；

[0029] 接收并根据所述第一终端发送的第一加密梯度值和所述第二终端发送的第二加密梯度值计算梯度和，根据所述梯度和更新所述第一加密联邦学习模型参数，得到第二加密联邦学习模型参数，将所述第二加密联邦学习模型参数发送给所述第一终端和所述第二终端；

[0030] 接收并根据所述第一终端发送的第三加密损失值和所述第二终端发送的第四加密损失值计算新的损失和，并根据所述新的损失和判断所述待训练联邦学习模型是否处于收敛状态，所述第三加密损失值由所述第一终端根据所述第一样本、所述第一加密补全样本以及所述第三终端发送的所述第二加密联邦学习模型参数计算得到，所述第四加密损失值由所述第二终端根据所述第二样本、所述第二加密补全样本以及所述第三终端发送的所述第二加密联邦学习模型参数计算得到；

[0031] 若所述待训练联邦学习模型处于收敛状态，则向所述第一终端和所述第二终端发送停止训练指令，并将所述第二加密联邦学习模型参数作为所述待训练联邦学习模型的最终参数。

[0032] 可选地，所述根据所述损失和判断所述待训练联邦学习模型是否处于收敛状态的步骤包括：

[0033] 根据所述损失和是否小于或者等于预设阈值，判断所述待训练联邦学习模型是否处于收敛状态；

[0034] 若所述损失和小于或者等于预设阈值，则判定所述待训练联邦学习模型处于收敛状态；

[0035] 若所述损失和大于预设阈值，则判定所述待训练联邦学习模型处于未收敛状态。

[0036] 此外，为实现上述目的，本发明还提出一种终端，所述终端为第一终端，所述第一终端包括：存储器、处理器及存储在所述存储器上并可在所述处理器上运行的基于联邦学习的模型参数训练程序，所述基于联邦学习的模型参数训练程序被所述处理器执行时实现如上所述的基于联邦学习的模型参数训练方法的步骤。

[0037] 本发明还提出一种终端，其特征在于，所述终端为第三终端，所述第三终端包括：存储器、处理器及存储在所述存储器上并可在所述处理器上运行的基于联邦学习的模型参数训练程序，所述基于联邦学习的模型参数训练程序被所述处理器执行时实现如上所述的基于联邦学习的模型参数训练方法的步骤。

[0038] 本发明还提出一种基于联邦学习的模型参数训练系统，所述基于联邦学习的模型参数训练系统包括至少一个如上所述的第一终端、至少一个如上所述的第三终端和至少一个能与所述第一终端和所述第三终端交互的第二终端。

[0039] 此外，为实现上述目的，本发明还提出一种存储介质，应用于计算机，所述存储介质上存储有基于联邦学习的模型参数训练程序，所述基于联邦学习的模型参数训练程序被处理器执行时实现如上所述的基于联邦学习的模型参数训练方法的步骤。

[0040] 本发明通过确定第一终端的第一样本与第二终端的第二样本的特征交集，基于特征交集训练第一样本得到第一映射模型，并发送给第二终端；接收第二终端发送的第二加密映射模型，并对第一样本缺失的特征部分进行预测得到第一加密补全样本；接收由第三终端发送的第一加密联邦学习模型参数，根据第一加密联邦学习模型参数训练待训练联邦学习模型，并计算第一加密损失值；将第一加密损失值发送给第三终端；在接收到第三终端发送的停止训练指令时，则将第一加密联邦学习模型参数作为待训练联邦学习模型的最终参数。本发明实现了利用迁移学习对联邦双方特征空间进行拓展，提高联邦模型的预测能力。

附图说明

[0041] 图1是本发明实施例方案涉及的硬件运行环境的结构示意图；

[0042] 图2为本发明基于联邦学习的模型参数训练方法第一实施例的流程示意图；

[0043] 图3为本发明基于联邦学习的模型参数训练方法第三实施例的场景示意图。

[0044] 本发明目的的实现、功能特点及优点将结合实施例，参照附图做进一步说明。

具体实施方式

[0045] 应当理解，此处所描述的具体实施例仅仅用以解释本发明，并不用于限定本发明。

[0046] 如图1所示，图1是本发明实施例方案涉及的硬件运行环境的终端结构示意图。

[0047] 需要说明的是，本发明实施例终端可以是智能手机、个人计算机和服务器等终端设备，在此不做具体限制。

[0048] 如图1所示，该模型参数训练装置可以包括：处理器1001，例如CPU，网络接口1004，用户接口1003，存储器1005，通信总线1002。其中，通信总线1002用于实现这些组件之间的连接通信。用户接口1003可以包括显示屏(Display)、输入单元比如键盘(Keyboard)，可选用户接口1003还可以包括标准的有线接口、无线接口。网络接口1004可选的可以包括标准

的有线接口、无线接口(如WI-FI接口)。存储器1005可以是高速RAM存储器,也可以是稳定的存储器(non-volatile memory),例如磁盘存储器。存储器1005可选的还可以是独立于前述处理器1001的存储装置。

[0049] 本领域技术人员可以理解,图1中示出的模型参数训练装置结构并不构成对模型参数训练装置的限定,可以包括比图示更多或更少的部件,或者组合某些部件,或者不同的部件布置。

[0050] 如图1所示,作为一种计算机存储介质的存储器1005中可以包括操作系统、网络通信模块、用户接口模块以及基于联邦学习的模型参数训练程序。其中,操作系统是管理和控制模型参数训练装置硬件和软件资源的程序,支持基于联邦学习的模型参数训练程序以及其它软件或程序的运行。

[0051] 在图1所示的模型参数训练装置中,用户接口1003主要用于与各个终端进行数据通信;网络接口1004主要用于连接后台服务器,与后台服务器进行数据通信;而处理器1001可以用于调用存储器1005中存储的基于联邦学习的模型参数训练程序,并执行以下操作:

[0052] 确定所述第一终端的第一样本与第二终端的第二样本的特征交集,基于所述特征交集训练所述第一样本得到第一映射模型,并将所述第一映射模型加密发送给所述第二终端,以供所述第二终端对所述第二样本缺失的特征部分进行预测得到第二加密补全样本;

[0053] 接收所述第二终端发送的第二加密映射模型,根据所述第二加密映射模型对所述第一终端的第一样本缺失的特征部分进行预测得到第一加密补全样本,所述第二加密映射模型是所述第二终端基于所述特征交集训练所述第二样本得到;

[0054] 接收由第三终端发送的第一加密联邦学习模型参数,根据所述第一加密联邦学习模型参数、所述第一样本与所述第一加密补全样本训练待训练联邦学习模型,并计算第一加密损失值;

[0055] 将所述第一加密损失值发送给第三终端,以供所述第三终端根据所述第一加密损失值与第二加密损失值计算损失和,根据所述损失和判断所述待训练联邦学习模型是否处于收敛状态,所述第二加密损失值由所述第二终端根据所述第二样本、所述第二加密补全样本以及所述第三终端发送的所述第一加密联邦学习模型参数计算得到;

[0056] 在接收到所述第三终端发送的停止训练指令时,则将所述第一加密联邦学习模型参数作为所述待训练联邦学习模型的最终参数,所述停止训练指令由所述第三终端在判定所述待训练联邦学习模型处于收敛状态后发出。

[0057] 进一步地,处理器1001还可以用于调用存储器1005中存储的基于联邦学习的模型参数训练程序,并执行以下步骤:

[0058] 基于所述待训练联邦学习模型的最终参数与所述第一样本或者所述第一加密补全样本计算得到第一加密预测结果,将所述第一加密预测结果发送给所述第三终端;

[0059] 在所述第三终端对所述第一加密预测结果解密后,获取所述第三终端解密得到的第一预测结果。

[0060] 进一步地,处理器1001还可以用于调用存储器1005中存储的基于联邦学习的模型参数训练程序,并执行以下步骤:

[0061] 在接收到所述第三终端发送的继续训练指令时,计算并将与所述第一加密损失值对应的第一加密梯度值发送给所述第三终端,以供所述第三终端根据所述第一加密梯度值

与第二加密梯度值计算梯度和，根据所述梯度和更新所述第一加密联邦学习模型参数，得到第二加密联邦学习模型参数，所述第二加密梯度值由所述第二终端根据所述第二样本、所述第二加密补全样本以及所述第三终端发送的所述第一加密联邦学习模型参数计算得到，所述继续训练指令由所述第三终端在判定所述待训练联邦学习模型处于未收敛状态时发出；

[0062] 获取由所述第三终端发送的所述第二加密联邦学习模型参数，并根据所述第二加密联邦学习模型参数计算所述第一终端的第三加密损失值；

[0063] 将所述第三加密损失值发送给第三终端，以供所述第三终端根据所述第三加密损失值与第四加密损失值计算新的损失和，根据所述新的损失和判断所述待训练联邦学习模型是否处于收敛状态，所述第四加密损失值由所述第二终端根据所述第二样本、所述第二加密补全样本以及所述第三终端发送的所述第二加密联邦学习模型参数计算得到；

[0064] 在接收到所述第三终端发送的停止训练指令时，则将所述第二加密联邦学习模型参数作为所述待训练联邦学习模型的最终参数。

[0065] 进一步地，处理器1001还可以用于调用存储器1005中存储的基于联邦学习的模型参数训练程序，并执行以下步骤：

[0066] 在第一终端利用第二终端的第二加密映射模型对所述第一终端的第一样本缺失的特征部分进行预测得到第一加密补全样本，所述第二终端利用所述第一终端的第一加密映射模型对所述第二终端的第二样本缺失的特征部分进行预测得到第二加密补全样本之后，所述第三终端向所述第一终端和所述第二终端发送第一加密联邦学习模型参数，以供所述第一终端根据所述第一加密联邦学习模型参数、所述第一样本与所述第一加密补全样本计算第一加密损失值，以及所述第二终端根据所述第一加密联邦学习模型参数、所述第二样本与所述第二加密补全样本计算第二加密损失值，其中，所述第二加密映射模型由所述第一样本与所述第二样本的特征交集训练所述第二样本得到，所述第一加密映射模型由所述特征交集训练所述第一样本得到；

[0067] 接收并根据由所述第一终端发送的所述第一加密损失值与由所述第二终端发送的所述第二加密损失值计算损失和，并根据所述损失和判断所述待训练联邦学习模型是否处于收敛状态；

[0068] 若所述待训练联邦学习模型处于收敛状态，则将所述第一加密联邦学习模型参数作为所述待训练联邦学习模型的最终参数。

[0069] 进一步地，处理器1001还可以用于调用存储器1005中存储的基于联邦学习的模型参数训练程序，并执行以下步骤：

[0070] 接收到所述第一终端发送的第一加密预测结果；

[0071] 解密所述第一加密预测结果得到第一预测结果，将解密得到的所述第一预测结果发送给所述第一终端。

[0072] 进一步地，处理器1001还可以用于调用存储器1005中存储的基于联邦学习的模型参数训练程序，并执行以下步骤：

[0073] 若判定所述待训练联邦学习模型处于未收敛状态，则向所述第一终端和所述第二终端发送继续训练指令；

[0074] 接收并根据所述第一终端发送的第一加密梯度值和所述第二终端发送的第二加

密梯度值计算梯度和，根据所述梯度和更新所述第一加密联邦学习模型参数，得到第二加密联邦学习模型参数，将所述第二加密联邦学习模型参数发送给所述第一终端和所述第二终端；

[0075] 接收并根据所述第一终端发送的第三加密损失值和所述第二终端发送的第四加密损失值计算新的损失和，并根据所述新的损失和判断所述待训练联邦学习模型是否处于收敛状态，所述第三加密损失值由所述第一终端根据所述第一样本、所述第一加密补全样本以及所述第三终端发送的所述第二加密联邦学习模型参数计算得到，所述第四加密损失值由所述第二终端根据所述第二样本、所述第二加密补全样本以及所述第三终端发送的所述第二加密联邦学习模型参数计算得到；

[0076] 若所述待训练联邦学习模型处于收敛状态，则向所述第一终端和所述第二终端发送停止训练指令，并将所述第二加密联邦学习模型参数作为所述待训练联邦学习模型的最终参数。

[0077] 进一步地，处理器1001还可以用于调用存储器1005中存储的基于联邦学习的模型参数训练程序，并执行以下步骤：

[0078] 根据所述损失和是否小于或者等于预设阈值，判断所述待训练联邦学习模型是否处于收敛状态；

[0079] 若所述损失和小于或者等于预设阈值，则判定所述待训练联邦学习模型处于收敛状态；

[0080] 若所述损失和大于预设阈值，则判定所述待训练联邦学习模型处于未收敛状态。

[0081] 本发明提供的技术方案，所述终端通过处理器1001调用存储器1005中存储的基于联邦学习的模型参数训练程序，以实现步骤：确定第一终端的第一样本与第二终端的第二样本的特征交集，基于特征交集训练第一样本得到第一映射模型，并发送给第二终端；接收第二终端发送的第二加密映射模型，并对第一样本缺失的特征部分进行预测得到第一加密补全样本；接收由第三终端发送的第一加密联邦学习模型参数，根据第一加密联邦学习模型参数训练待训练联邦学习模型，并计算第一加密损失值；将第一加密损失值发送给第三终端；在接收到第三终端发送的停止训练指令时，则将第一加密联邦学习模型参数作为待训练联邦学习模型的最终参数。本发明实现了利用迁移学习对联邦双方特征空间进行拓展，提高联邦模型的预测能力。

[0082] 此外，本发明实施例还提出一种终端，所述终端为第一终端，所述第一终端包括：存储器、处理器及存储在所述存储器上并可在所述处理器上运行的基于联邦学习的模型参数训练程序，所述基于联邦学习的模型参数训练程序被所述处理器执行时实现如上所述的基于联邦学习的模型参数训练方法的步骤。

[0083] 其中，在所述处理器上运行的基于联邦学习的模型参数训练程序被执行时所实现的方法可参照本发明基于联邦学习的模型参数训练方法各个实施例，此处不再赘述。

[0084] 此外，本发明实施例还提出一种终端，所述终端为第三终端，所述第三终端包括：存储器、处理器及存储在所述存储器上并可在所述处理器上运行的基于联邦学习的模型参数训练程序，所述基于联邦学习的模型参数训练程序被所述处理器执行时实现如上所述的基于联邦学习的模型参数训练方法的步骤。

[0085] 其中，在所述处理器上运行的基于联邦学习的模型参数训练程序被执行时所实现

的方法可参照本发明基于联邦学习的模型参数训练方法各个实施例，此处不再赘述。

[0086] 此外，本发明实施例还提出一种基于联邦学习的模型参数训练系统，其特征在于，所述基于联邦学习的模型参数训练系统至少一个如上所述的第一终端、至少一个如上所述的第三终端和至少一个能与所述第一终端和所述第三终端交互的第二终端。

[0087] 此外，本发明实施例还提出一种计算机可读存储介质，所述存储介质上存储有基于联邦学习的模型参数训练程序，所述基于联邦学习的模型参数训练程序被处理器执行时实现如上所述的基于联邦学习的模型参数训练方法的步骤。

[0088] 其中，在所述处理器上运行的基于联邦学习的模型参数训练程序被执行时所实现的方法可参照本发明基于联邦学习的模型参数训练方法各个实施例，此处不再赘述。

[0089] 基于上述的结构，提出基于联邦学习的模型参数训练方法的各个实施例。

[0090] 参照图2，图2为本发明基于联邦学习的模型参数训练方法第一实施例的流程示意图。

[0091] 本发明实施例提供了基于联邦学习的模型参数训练方法的实施例，需要说明的是，虽然在流程图中示出了逻辑顺序，但是在某些情况下，可以以不同于此处的顺序执行所示出或描述的步骤。

[0092] 本发明第一实施例基于联邦学习的模型参数训练方法应用于第一终端，本发明实施例第一终端、第二终端和第三终端可以是智能手机、个人计算机和服务器等终端设备，在此不做具体限制。

[0093] 本实施例基于联邦学习的模型参数训练方法包括：

[0094] 步骤S1，确定所述第一终端的第一样本与第二终端的第二样本的特征交集，基于所述特征交集训练所述第一样本得到第一映射模型，并将所述第一映射模型加密发送给所述第二终端，以供所述第二终端对所述第二样本缺失的特征部分进行预测得到第二加密补全样本；

[0095] “机器学习”是人工智能的核心研究领域之一，而如何在保护数据隐私、满足合法合规要求的前提下继续进行机器学习，是机器学习领域现在关注的一个趋势，在此背景下，人们研究提出了“联邦学习”的概念。

[0096] 联邦学习利用技术算法加密建造的模型，联邦双方在不用给出己方数据的情况下，也可进行模型训练得到模型参数，联邦学习通过加密机制下的参数交换方式保护用户数据隐私，数据和模型本身不会进行传输，也不能反猜对方数据，因此在数据层面不存在泄露的可能，也不违反更严格的数据保护法案如GDPR(General Data Protection Regulation，《通用数据保护条例》)等，能够在较高程度保持数据完整性的同时，保障数据隐私。

[0097] 但目前现有的横向联邦方法只能应用在联邦双方A、B样本均有标注，且双方的特征维度相同的情况，而对于A、B双方特征维度不同的情况不适用。为了解决这一问题，提出本发明基于联邦学习的模型参数训练方法的各个实施例。

[0098] 本发明基于横向联邦学习，横向联邦学习是指在两个数据集(即可以是本发明实施例中所述的第一样本和第二样本)的用户特征重叠较多，而用户重叠较少的情况下，把数据集按照横向(即用户维度)切分，并取出双方用户特征相同而用户不完全相同的那部分数据进行训练。这种方法叫做横向联邦学习。比如有两家不同地区的银行，它们的用户群体分

别来自各自所在的地区，相互的交集很小。但是，它们的业务很相似，因此，记录的用户特征是相同的。

[0099] 本实施例中，第一终端的第一样本和第二终端的第二样本的样本维度不同，特征维度有部分重叠。

[0100] 首先第一终端确定第一样本与第二样本的特征维度的重叠部分，基于该重叠部分的交集，将第一样本的非重叠部分与该重叠部分进行训练得到从重叠部分到非重叠部分的函数映射模型，即第一映射模型，并将该第一映射模型通过预设加密算法加密得到第一加密映射模型后发送给第二终端，第二终端在接收到该第一加密映射模型后，利用该第一加密映射模型对第二样本缺失的特征部分进行预测，得到第二加密补全样本。

[0101] 其中，预设加密算法为同态加密算法(Homomorphic Encryption)。

[0102] 步骤S2，接收所述第二终端发送的第二加密映射模型，根据所述第二加密映射模型对所述第一终端的第一样本缺失的特征部分进行预测得到第一加密补全样本，所述第二加密映射模型是所述第二终端基于所述特征交集训练所述第二样本得到；

[0103] 同时，第二终端确定第一样本与第二样本的特征维度的重叠部分，基于该重叠部分的交集，将第二样本的非重叠部分与该重叠部分进行训练得到从重叠部分到非重叠部分的函数映射模型，即第二映射模型，并将该第二映射模型通过预设加密算法加密得到第二加密映射模型后发送给第一终端，第一终端在接收到该第二加密映射模型后，利用该第二加密映射模型对第一样本缺失的特征部分进行预测，得到第一加密补全样本。

[0104] 其中，预设加密算法为同态加密算法(Homomorphic Encryption)。

[0105] 步骤S3，接收由第三终端发送的第一加密联邦学习模型参数，根据所述第一加密联邦学习模型参数、所述第一样本与所述第一加密补全样本训练待训练联邦学习模型，并计算第一加密损失值；

[0106] 在第一终端和第二终端分别对各自缺失的特征部分进行预测补全之后，基于第一终端和第二终端的完整的数据进行横向联邦学习建模，即待训练联邦学习模型。第三终端将该待训练联邦学习模型的第一加密联邦学习模型参数分别发送给第一终端和第二终端，以供第一终端根据该第一加密联邦学习模型参数、第一样本和第一加密补全样本训练待训练联邦学习模型，并计算加密损失值，作为第一加密损失值，同时，第二终端根据该第一加密联邦学习模型参数、第二样本和第二补全样本训练待训练联邦学习模型，并计算加密损失值，作为第二加密损失值。

[0107] 步骤S4，将所述第一加密损失值发送给第三终端，以供所述第三终端根据所述第一加密损失值与第二加密损失值计算损失和，根据所述损失和判断所述待训练联邦学习模型是否处于收敛状态，所述第二加密损失值由所述第二终端根据所述第二样本、所述第二加密补全样本以及所述第三终端发送的所述第一加密联邦学习模型参数计算得到；

[0108] 在第一终端和第二终端根据第一加密联邦学习模型参数各自计算出第一加密损失值和第二加密损失值之后，将第一加密损失值和第二加密损失值发送给第三终端，第三终端在接收到第一加密损失值和第二加密损失值后，根据第一加密损失值和第二加密损失值计算损失和有两种实现方式，一种是第三终端先通过预设解密算法对第一加密损失值和第二加密损失值进行解密，得到第一损失值和第二损失值，再计算第一损失值和第二损失值的和，作为损失和；另一种实现方式是第三终端先对第一加密损失值和第二加密损失值

求和，得到加密损失和，再通过预设解密算法对加密损失和进行解密得到损失和。

[0109] 以上两种实现方式择其一即可，具体选择本实施例不做限制。

[0110] 得到损失和后，第三终端再根据损失和判断该待训练联邦学习模型是否处于收敛状态。

[0111] 具体地，若损失和小于或者等于预设阈值，则判定待训练联邦学习模型处于收敛状态，若损失和大于预设阈值，则判定待训练联邦学习模型处于未收敛状态。

[0112] 其中，预设阈值的大小用户或者运维人员可根据需要设置，本实施例不做限制。

[0113] 步骤S5，在接收到所述第三终端发送的停止训练指令时，则将所述第一加密联邦学习模型参数作为所述待训练联邦学习模型的最终参数，所述停止训练指令由所述第三终端在判定所述待训练联邦学习模型处于收敛状态后发出。

[0114] 在第三终端判定待训练联邦学习模型处于收敛状态时，则向第一终端和第二终端发送停止训练指令，并将该第一加密联邦学习模型参数作为待训练联邦学习模型的最终参数，即最优参数，第一终端和第二终端在接收到该停止训练指令时，将该第一加密联邦学习模型参数作为待训练联邦学习模型的最终参数。

[0115] 本实施例中，第三终端根据解密后的损失和检测到所述待训练联邦学习模型处于收敛状态，并将对应的第一加密联邦学习模型参数作为所述待训练联邦学习模型的最终参数，待训练联邦学习模型训练完成。

[0116] 进一步地，在本发明基于联邦学习的模型参数训练方法的第二实施例中，上述步骤S4之后还包括：

[0117] 步骤S41，在接收到所述第三终端发送的继续训练指令时，计算并将与所述第一加密损失值对应的第一加密梯度值发送给所述第三终端，以供所述第三终端根据所述第一加密梯度值与第二加密梯度值计算梯度和，根据所述梯度和更新所述第一加密联邦学习模型参数，得到第二加密联邦学习模型参数，所述第二加密梯度值由所述第二终端根据所述第二样本、所述第二加密补全样本以及所述第三终端发送的所述第一加密联邦学习模型参数计算得到，所述继续训练指令由所述第三终端在判定所述待训练联邦学习模型处于未收敛状态时发出；

[0118] 在第三终端判定待训练联邦学习模型处于未收敛状态时，则向第一终端和第二终端发送继续训练指令，在第一终端接收到继续训练指令时，计算并将于与第一加密损失值对应的第一加密梯度值发送给第三终端，同时，在第二终端接收到继续训练指令时，计算并将于与第二加密损失值对应的第二加密梯度值发送给第三终端。

[0119] 本实施例还有一种实施方式，第一终端和第二终端在上次向第三终端发送加密损失值的时候同时将加密梯度值发送给第三终端，在第三终端判定待训练联邦学习模型处于未收敛状态时，则计算加密梯度和并解密得到梯度和，第三终端根据该梯度和更新第一加密联邦学习模型参数，得到第二加密联邦学习模型参数。

[0120] 以上两种发送加密梯度值给第三终端的实施方式择其一即可，具体选择本实施例不做限制。

[0121] 步骤S42，获取由所述第三终端发送的所述第二加密联邦学习模型参数，并根据所述第二加密联邦学习模型参数计算所述第一终端的第三加密损失值；

[0122] 第三终端在接收到第一加密梯度值和第二加密梯度值后，根据第一加密梯度值和

第二加密梯度值计算梯度和有两种实现方式，一种是第三终端先通过预设解密算法对第一加密梯度值和第二加密梯度值进行解密，得到第一梯度值和第二梯度值，再计算第一梯度值和第二梯度值的和，作为梯度和；另一种实现方式是第三终端先对第一加密梯度值和第二加密梯度值求和，得到加密梯度和，再通过预设解密算法对加密梯度和进行解密得到梯度和。

[0123] 以上两种实现方式择其一即可，具体选择本实施例不做限制。

[0124] 得到梯度和后，第三终端根据该梯度和更新第一加密联邦学习模型参数，得到第二加密联邦学习模型参数，并将第二加密联邦学习模型参数发送给第一终端和第二终端。

[0125] 第一终端获取第三终端发送的第二加密联邦学习模型参数，并根据第二加密联邦学习模型参数计算第一终端的新的加密损失值，即第三加密损失值，对应的，第二终端获取第三终端发送的第二加密联邦学习模型参数，并根据第二加密联邦学习模型参数计算第二终端的新的加密损失值，即第四加密损失值。

[0126] 步骤S43，将所述第三加密损失值发送给第三终端，以供所述第三终端根据所述第三加密损失值与第四加密损失值的损失和判断所述待训练联邦学习模型是否处于收敛状态，所述第四加密损失值由所述第二终端根据所述第二样本、所述第二加密补全样本以及所述第三终端发送的所述第二加密联邦学习模型参数计算得到；

[0127] 第一终端和第二终端在根据第二加密联邦学习模型参数计算得到第三加密损失值和第四加密损失值后，将第三加密损失值和第四加密损失值后各自发给第三终端，第三终端在接收到第一终端和第二终端发送的第三加密损失值和第四加密损失值后，计算第三加密损失值和第四加密损失值的损失和，得到新的损失和，第三终端再根据该新的损失和判断该待训练联邦学习模型是否处于收敛状态。具体地，若损失和小于或者等于预设阈值，则判定待训练联邦学习模型处于收敛状态，若损失和大于预设阈值，则判定待训练联邦学习模型处于未收敛状态。

[0128] 其中，预设阈值的大小用户或者运维人员可根据需要设置，本实施例不做限制。

[0129] 步骤S44，在接收到所述第三终端发送的停止训练指令时，则将所述第二加密联邦学习模型参数作为所述待训练联邦学习模型的最终参数。

[0130] 在第三终端判定待训练联邦学习模型处于收敛状态时，则向第一终端和第二终端发送停止训练指令，并将该第二加密联邦学习模型参数作为待训练联邦学习模型的最终参数，即最优参数，第一终端和第二终端在接收到该停止训练指令时，将该第二加密联邦学习模型参数作为待训练联邦学习模型的最终参数。

[0131] 进一步地，上述步骤S5之后还包括：

[0132] 步骤S51，基于所述待训练联邦学习模型的最终参数与所述第一样本或者所述第一加密补全样本计算得到第一加密预测结果，将所述第一加密预测结果发送给所述第三终端；

[0133] 在确定了待训练联邦学习模型的最优参数之后，第一终端和第二终端都可以使用该最优参数，但此最优参数是加密的，第一终端可以通过第一样本、第一加密补全样本和加密的最优参数得到第一加密预测结果，将该第一加密预测结果发送给第三终端解密。

[0134] 步骤S52，在所述第三终端对所述第一加密预测结果解密后，获取所述第三终端解密得到的第一预测结果。

[0135] 第三终端解密在接收到第一加密预测结果后，通过预设解密算法对其进行解密，得到第一预测结果，将其发送给第一终端。对应的，第二终端也可以与第一终端执行相似的步骤。

[0136] 本实施例通过在接收到所述第三终端发送的继续训练指令时，计算并将与所述第一加密损失值对应的第一加密梯度值发送给所述第三终端，以供所述第三终端根据所述第一加密梯度值与第二加密梯度值计算梯度和，根据所述梯度和更新所述第一加密联邦学习模型参数，得到第二加密联邦学习模型参数；获取由所述第三终端发送的所述第二加密联邦学习模型参数，得到第二加密联邦学习模型参数，并根据所述第二加密联邦学习模型参数计算所述第一终端的第三加密损失值；将所述第三加密损失值发送给第三终端，以供所述第三终端根据所述第三加密损失值与第四加密损失值计算新的损失和，根据所述新的损失和判断所述待训练联邦学习模型是否处于收敛状态；在接收到所述第三终端发送的停止训练指令时，则将所述第二加密联邦学习模型参数作为所述待训练联邦学习模型的最终参数。实现了第三终端联合第一终端和第二终端的样本数据计算得到损失和，以通过联合第一终端和第二终端的样本数据联合帮助学习确定待训练联邦学习模型中的模型参数，提高了训练所得模型的准确度。

[0137] 进一步地，提出本发明基于联邦学习的模型参数获取方法第三实施例，在本实施例中，所述基于联邦学习的模型参数训练方法应用于第三终端，所述基于联邦学习的模型参数训练方法包括以下步骤：

[0138] 步骤C1，在第一终端利用第二终端的第二加密映射模型对所述第一终端的第一样本缺失的特征部分进行预测得到第一加密补全样本，所述第二终端利用所述第一终端的第一加密映射模型对所述第二终端的第二样本缺失的特征部分进行预测得到第二加密补全样本之后，所述第三终端向所述第一终端和所述第二终端发送第一加密联邦学习模型参数，以供所述第一终端根据所述第一加密联邦学习模型参数、所述第一样本与所述第一加密补全样本计算第一加密损失值，以及所述第二终端根据所述第一加密联邦学习模型参数、所述第二样本与所述第二加密补全样本计算第二加密损失值，其中，所述第二加密映射模型由所述第一样本与所述第二样本的特征交集训练所述第二样本得到，所述第一加密映射模型由所述特征交集训练所述第一样本得到；

[0139] 在本实施例中，第一终端的第一样本和第二终端的第二样本的样本维度不同，特征维度有部分重叠。

[0140] 首先第一终端确定第一样本与第二样本的特征维度的重叠部分，基于该重叠部分的交集，将第一样本的非重叠部分与该重叠部分进行训练得到从重叠部分到非重叠部分的函数映射模型，即第一映射模型，并将该第一映射模型通过预设加密算法加密得到第一加密映射模型后发送给第二终端，第二终端在接收到该第一加密映射模型后，利用该第一加密映射模型对第二样本缺失的特征部分进行预测，得到第二加密补全样本。

[0141] 同时，第二终端确定第一样本与第二样本的特征维度的重叠部分，基于该重叠部分的交集，将第二样本的非重叠部分与该重叠部分进行训练得到从重叠部分到非重叠部分的函数映射模型，即第二映射模型，并将该第二映射模型通过预设加密算法加密得到第二加密映射模型后发送给第一终端，第一终端在接收到该第二加密映射模型后，利用该第二加密映射模型对第一样本缺失的特征部分进行预测，得到第一加密补全样本。

[0142] 其中，预设加密算法为同态加密算法(Homomorphic Encryption)。

[0143] 在第一终端和第二终端分别对各自缺失的特征部分进行预测补全之后，基于第一终端和第二终端的完整的数据进行横向联邦学习建模，即待训练联邦学习模型。第三终端将该待训练联邦学习模型的第一加密联邦学习模型参数分别发送给第一终端和第二终端，以供第一终端根据该第一加密联邦学习模型参数、第一样本和第一加密补全样本训练待训练联邦学习模型，并计算加密损失值，作为第一加密损失值，同时，第二终端根据该第一加密联邦学习模型参数、第二样本和第二补全样本训练待训练联邦学习模型，并计算加密损失值，作为第二加密损失值。

[0144] 步骤C2，接收并根据由所述第一终端发送的所述第一加密损失值与由所述第二终端发送的所述第二加密损失值计算损失和，并根据所述损失和判断所述待训练联邦学习模型是否处于收敛状态；

[0145] 在第一终端和第二终端根据第一加密联邦学习模型参数各自计算出第一加密损失值和第二加密损失值之后，将第一加密损失值和第二加密损失值发送给第三终端，第三终端在接收到第一加密损失值和第二加密损失值后，根据第一加密损失值和第二加密损失值计算损失和有两种实现方式，一种是第三终端先通过预设解密算法对第一加密损失值和第二加密损失值进行解密，得到第一损失值和第二损失值，再计算第一损失值和第二损失值的和，作为损失和；另一种实现方式是第三终端先对第一加密损失值和第二加密损失值求和，得到加密损失和，再通过预设解密算法对加密损失和进行解密得到损失和。

[0146] 以上两种实现方式择其一即可，具体选择本实施例不做限制。

[0147] 得到损失和后，第三终端再根据损失和判断该待训练联邦学习模型是否处于收敛状态。

[0148] 步骤C3，若所述待训练联邦学习模型处于收敛状态，则将所述第一加密联邦学习模型参数作为所述待训练联邦学习模型的最终参数。

[0149] 若损失和小于或者等于预设阈值，则第三终端判定待训练联邦学习模型处于收敛状态，则向第一终端和第二终端发送停止训练指令，并将该第一加密联邦学习模型参数作为待训练联邦学习模型的最终参数，即最优参数，第一终端和第二终端在接收到该停止训练指令时，将该第一加密联邦学习模型参数作为待训练联邦学习模型的最终参数。

[0150] 为辅助理解，现列举一实例：如图3所示，A，B双方的样本维度不同，特征有部分重叠。B方有标注数据(X^B,Y^B)，A方有标注数据(X^A,Y^A).系统由A，B，C三方组成。C方产生加密公钥和私钥，并对从A,B两方传来的加密信息基于私钥进行解密。训练前，C方将公钥分发给A跟B。首先A方和B方确定双方的交集特征部分X_2^A， X_2^B。在A方，我们定义$X_1^A=\{X_{1,j}^A\}_{j=1}^n$为n个特征的集合。对每一个特征$X_{1,j}^A$，训练一个从$X_2^A$到$X_{1,j}^A$的函数映射模型$f_j^A:X_2^A\to X_{1,j}^A$。函数映射模型通过训练以下目标函数得到：

[0151] $$\min L(X_{1,j}^A, f_j^A(X_2^A,\theta_j^A))+\gamma\left\|\theta_j^A\right\|_F^2$$

[0152] 同理，在B方，我们定义$X_3^B=\{X_{3,k}^B\}_{k=1}^m$为m个特征的集合。对每一个特征$X_{3,k}^B$，训练一个从$X_2^B$到$X_{3,k}^B$的函数映射模型$f_k^B:X_2^B\to X_{3,k}^B$。函数映射模型通过训练以下目标函数得到：

[0153] $$\min L(X_{3,k}^{B}, f_k^{B}(X_2^{B}, \theta_k^{B})) + \gamma \left\| \theta_k^{B} \right\|_F^2$$

[0154] A,B两方进行特征补全,A方将加密模型$\{\!\{f_j^{A}\}\!\}_{j=1}^{n}$传给B方。B方利用$\{\!\{f_j^{A}\}\!\}_{j=1}^{n}$对缺失的特征$X_1^{B}$进行预测得到$[[X_1^{B}]]$。同理,B方将加密模型$\{\!\{f_k^{B}\}\!\}_{k=1}^{m}$传给A方,A方利用$\{\!\{f_k^{B}\}\!\}_{k=1}^{m}$对缺失的特征$X_3^{A}$进行预测得到$[[X_3^{A}]]$。

[0155] 随后,A,B两方进行横向联邦学习,C方初始化模型参数W,并将W加密得到[[W]],然后将[[W]]传给A和B方。A,B双方根据[[W]]分别计算加密损失$[[1^{A}]]$,$[[1^{B}]]$,并将加密的损失传给C方,C方解密损失,并将损失汇总加和,得到1^{C}。C根据损失值1^{C}判断是否收敛。若收敛,则结束训练。并将[[W]]作为最终参数。

[0156] 其中,L指损失函数,θ指模型参数,λ指正则式参数,F指平方和。

[0157] 本实施例中,第三终端根据解密后的损失和检测到所述待训练联邦学习模型处于收敛状态,并将对应的第一加密联邦学习模型参数作为所述待训练联邦学习模型的最终参数,待训练联邦学习模型训练完成。

[0158] 进一步地,所述根据所述损失和判断所述待训练联邦学习模型是否处于收敛状态的步骤包括:

[0159] 步骤C21,根据所述损失和是否小于或者等于预设阈值,判断所述待训练联邦学习模型是否处于收敛状态;

[0160] 步骤C22,若所述损失和小于或者等于预设阈值,则判定所述待训练联邦学习模型处于收敛状态;

[0161] 步骤C23,若所述损失和大于预设阈值,则判定所述待训练联邦学习模型处于未收敛状态。

[0162] 具体地,若损失和小于或者等于预设阈值,则判定待训练联邦学习模型处于收敛状态,若损失和大于预设阈值,则判定待训练联邦学习模型处于未收敛状态。

[0163] 其中,预设阈值的大小用户或者运维人员可根据需要设置,本实施例不做限制。

[0164] 进一步地,上述步骤C2之后还包括:

[0165] 步骤C201,若判定所述待训练联邦学习模型处于未收敛状态,则向所述第一终端和所述第二终端发送继续训练指令;

[0166] 在第三终端判定待训练联邦学习模型处于未收敛状态时,则向第一终端和第二终端发送继续训练指令,在第一终端接收到继续训练指令时,计算并将于与第一加密损失值对应的第一加密梯度值发送给第三终端,同时,在第二终端接收到继续训练指令时,计算并将于与第二加密损失值对应的第二加密梯度值发送给第三终端。

[0167] 步骤C202,接收并根据所述第一终端发送的第一加密梯度值和所述第二终端发送的第二加密梯度值计算梯度和,根据所述梯度和更新所述第一加密联邦学习模型参数,得到第二加密联邦学习模型参数,将所述第二加密联邦学习模型参数发送给所述第一终端和所述第二终端;

[0168] 第三终端在接收到第一加密梯度值和第二加密梯度值后,根据第一加密梯度值和第二加密梯度值计算梯度和有两种实现方式,一种是第三终端先通过预设解密算法对第一

加密梯度值和第二加密梯度值进行解密，得到第一梯度值和第二梯度值，再计算第一梯度值和第二梯度值的和，作为梯度和；另一种实现方式是第三终端先对第一加密梯度值和第二加密梯度值求和，得到加密梯度和，再通过预设解密算法对加密梯度和进行解密得到梯度和。

[0169] 以上两种实现方式择其一即可，具体选择本实施例不做限制。

[0170] 得到梯度和后，第三终端根据该梯度和更新第一加密联邦学习模型参数，得到第二加密联邦学习模型参数，并将第二加密联邦学习模型参数发送给第一终端和第二终端。

[0171] 步骤C203，接收并根据所述第一终端发送的第三加密损失值和所述第二终端发送的第四加密损失值计算新的损失和，并根据所述新的损失和判断所述待训练联邦学习模型是否处于收敛状态，所述第三加密损失值由所述第一终端根据所述第一样本、所述第一加密补全样本以及所述第三终端发送的所述第二加密联邦学习模型参数计算得到，所述第四加密损失值由所述第二终端根据所述第二样本、所述第二加密补全样本以及所述第三终端发送的所述第二加密联邦学习模型参数计算得到；

[0172] 第一终端获取第三终端发送的第二加密联邦学习模型参数，并根据第二加密联邦学习模型参数计算第一终端的新的加密损失值，即第三加密损失值，对应的，第二终端获取第三终端发送的第二加密联邦学习模型参数，并根据第二加密联邦学习模型参数计算第二终端的新的加密损失值，即第四加密损失值。

[0173] 第一终端和第二终端在根据第二加密联邦学习模型参数计算得到第三加密损失值和第四加密损失值后，将第三加密损失值和第四加密损失值后各自发给第三终端，第三终端在接收到第一终端和第二终端发送的第三加密损失值和第四加密损失值后，计算第三加密损失值和第四加密损失值的加密损失和，通过预设解密算法解密得到新的损失和，第三终端再根据该新的损失和判断该待训练联邦学习模型是否处于收敛状态。具体地，若损失和小于或者等于预设阈值，则判定待训练联邦学习模型处于收敛状态，若损失和大于预设阈值，则判定待训练联邦学习模型处于未收敛状态。

[0174] 其中，预设阈值的大小用户或者运维人员可根据需要设置，本实施例不做限制。

[0175] 步骤C204，若所述待训练联邦学习模型处于收敛状态，则向所述第一终端和所述第二终端发送停止训练指令，并将所述第二加密联邦学习模型参数作为所述待训练联邦学习模型的最终参数。

[0176] 在第三终端判定待训练联邦学习模型处于收敛状态时，则向第一终端和第二终端发送停止训练指令，并将该第二加密联邦学习模型参数作为待训练联邦学习模型的最终参数，即最优参数，第一终端和第二终端在接收到该停止训练指令时，将该第二加密联邦学习模型参数作为待训练联邦学习模型的最终参数。

[0177] A,B两方进行横向联邦学习，C方初始化模型参数W，并将W加密得到[[W]]，然后将[[W]]传给A和B方。A,B双方根据[[W]]分别计算加密损失$[[1^A]]$，$[[1^B]]$，并将加密的损失传给C，C方解密损失，并将损失汇总加和，得到1^C。C根据损失值1^C判断是否收敛。若没有收敛，C方获取与A,B双方根据[[W]]分别计算梯度$[[g^A]]$，$[[g^B]]$，并将加密的梯度传给C，C方求梯度和并解密梯度和得到g^C，C更新模型参数$W_1=W-\eta g^C$，加密W_1得到$[[W_1]]$，并将其传给A,B方。A,B方按照新的$[[W_1]]$计算新的加密损失值，并将其发送给C方，C方求和解密判断是否收敛，若收敛则向A和B发送停止训练指令，并将$[[W_1]]$作为最终参数。

[0178] 其中,η指学习率(learning rate),用户或者运维人员可预先设置η的大小,本实施例不做限制。

[0179] 进一步地,上述步骤C3之后还包括:

[0180] 步骤C31,接收到所述第一终端发送的第一加密预测结果;

[0181] 在确定了待训练联邦学习模型的最优参数之后,第一终端和第二终端都可以使用该最优参数,但此最优参数是加密的,第一终端可以通过第一样本、第一加密补全样本和加密的最优参数得到第一加密预测结果,将该第一加密预测结果发送给第三终端解密。

[0182] 步骤C32,解密所述第一加密预测结果得到第一预测结果,将解密得到的所述第一预测结果发送给所述第一终端。

[0183] 第三终端解密在接收到第一加密预测结果后,通过预设解密算法对其进行解密,得到第一预测结果,将其发送给第一终端。对应的,第二终端也可以与第一终端执行相似的步骤。

[0184] 本实施例实现了第三终端联合第一终端和第二终端的样本数据计算得到损失和,以通过联合第一终端和第二终端的样本数据联合帮助学习确定待训练联邦学习模型中的模型参数,提高了训练所得模型的准确度。

[0185] 需要说明的是,在本文中,术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含,从而使得包括一系列要素的过程、方法、物品或者装置不仅包括那些要素,而且还包括没有明确列出的其他要素,或者是还包括为这种过程、方法、物品或者装置所固有的要素。在没有更多限制的情况下,由语句“包括一个……”限定的要素,并不排除在包括该要素的过程、方法、物品或者装置中还存在另外的相同要素。

[0186] 上述本发明实施例序号仅仅为了描述,不代表实施例的优劣。

[0187] 通过以上的实施方式的描述,本领域的技术人员可以清楚地了解到上述实施例方法可借助软件加必需的通用硬件平台的方式来实现,当然也可以通过硬件,但很多情况下前者是更佳的实施方式。基于这样的理解,本发明的技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来,该计算机软件产品存储在一个存储介质(如ROM/RAM、磁碟、光盘)中,包括若干指令用以使得一台终端设备(可以是手机,计算机,服务器,空调器,或者网络设备等)执行本发明各个实施例所述的方法。

[0188] 以上仅为本发明的优选实施例,并非因此限制本发明的专利范围,凡是利用本发明说明书及附图内容所作的等效结构或等效流程变换,或直接或间接运用在其他相关的技术领域,均同理包括在本发明的专利保护范围内。

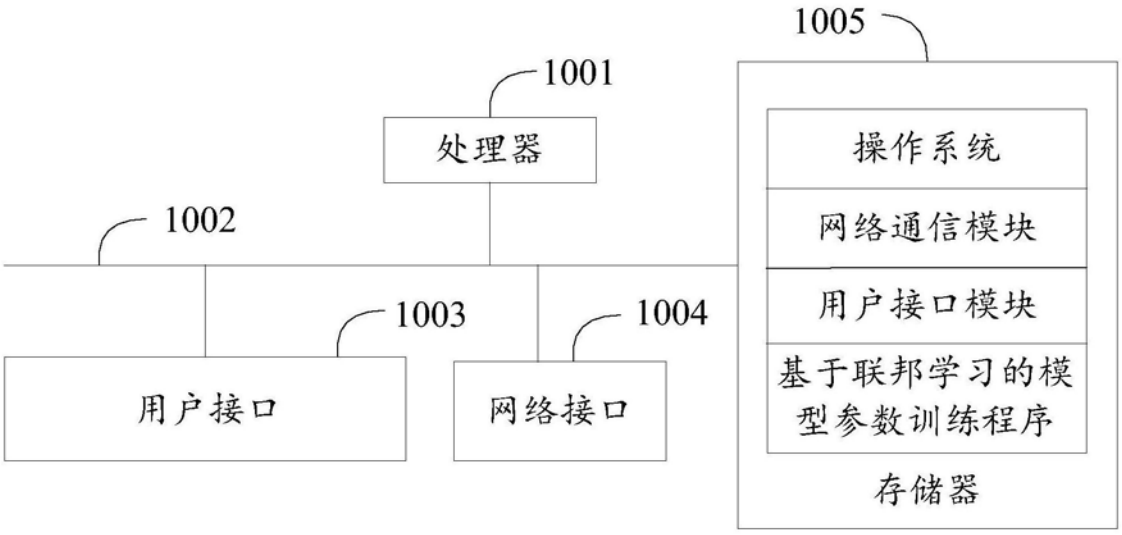

1005
1001
处理器
操作系统
网络通信模块
1002
用户接口模块
1003
1004
基于联邦学习的模型参数训练程序
用户接口
网络接口
存储器

图1

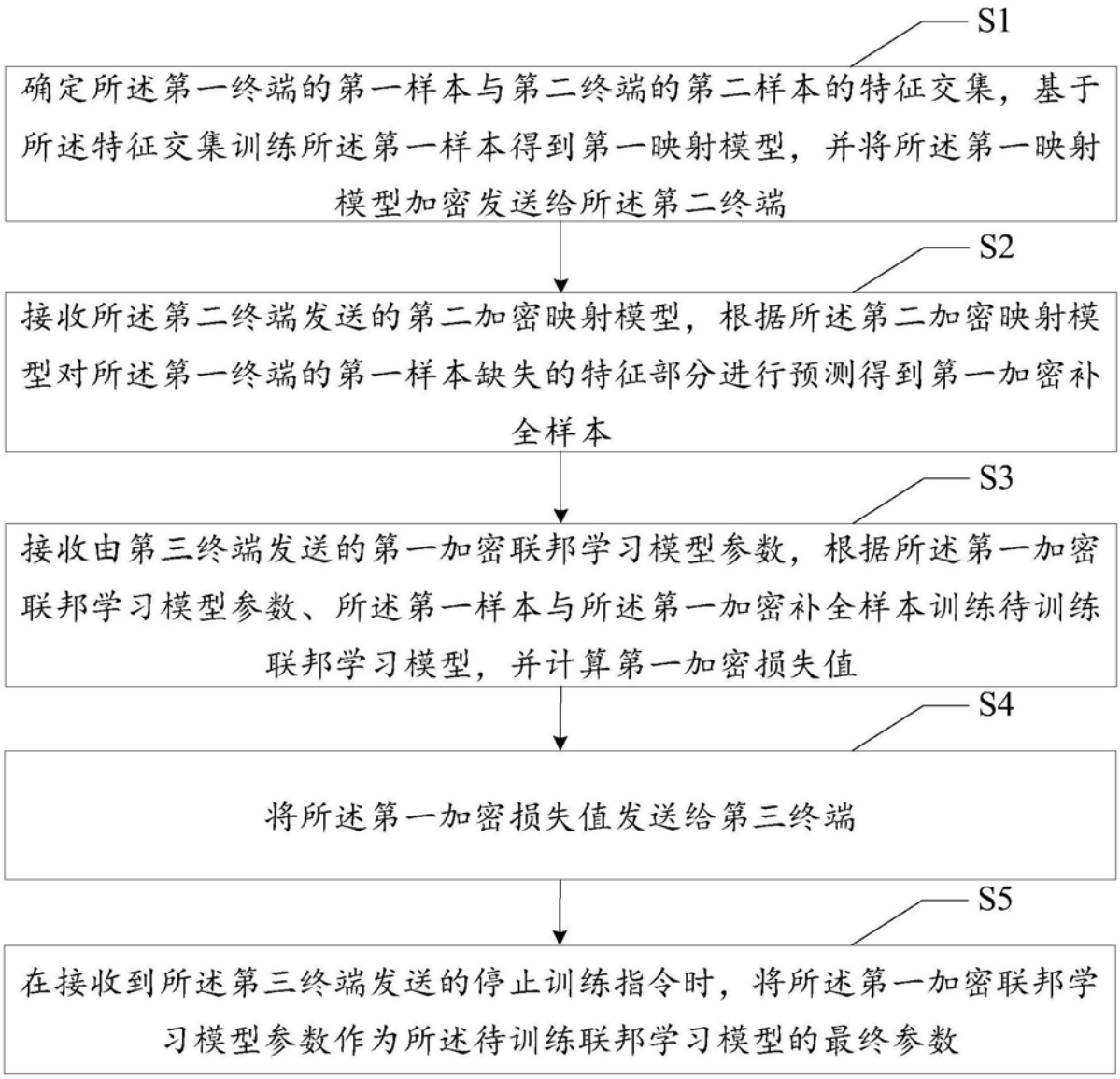

S1
确定所述第一终端的第一样本与第二终端的第二样本的特征交集，基于所述特征交集训练所述第一样本得到第一映射模型，并将所述第一映射模型加密发送给所述第二终端
S2
接收所述第二终端发送的第二加密映射模型，根据所述第二加密映射模型对所述第一终端的第一样本缺失的特征部分进行预测得到第一加密补全样本
S3
接收由第三终端发送的第一加密联邦学习模型参数，根据所述第一加密联邦学习模型参数、所述第一样本与所述第一加密补全样本训练待训练联邦学习模型，并计算第一加密损失值
S4
将所述第一加密损失值发送给第三终端
S5
在接收到所述第三终端发送的停止训练指令时，将所述第一加密联邦学习模型参数作为所述待训练联邦学习模型的最终参数

图2

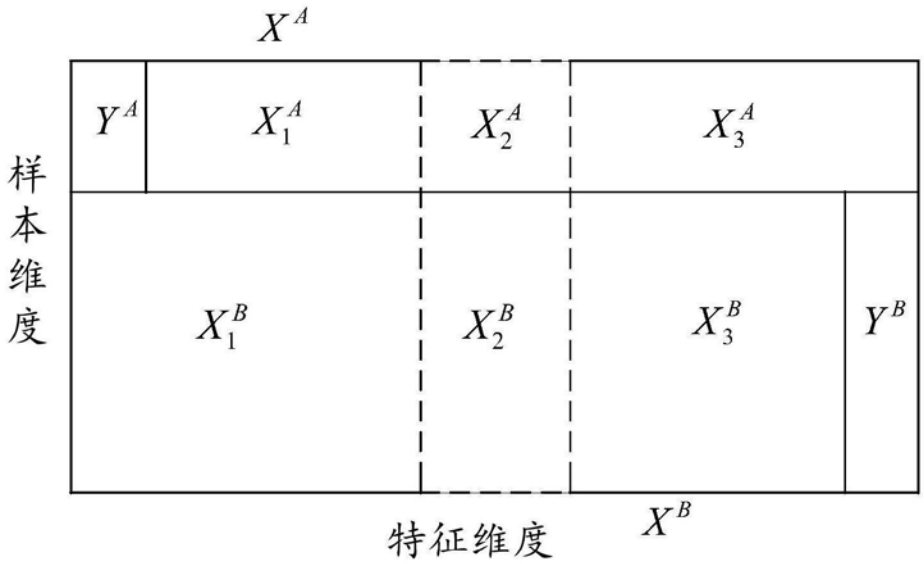


图3