(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 109871702 B
(45)授权公告日 2024.06.28

(21)申请号 201910121269.8
(22)申请日 2019.02.18
(65)同一申请的已公布的文献号
申请公布号 CN 109871702 A
(43)申请公布日 2019.06.11
(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 黄安埠 刘洋 陈天健 杨强
(74)专利代理机构 深圳市世纪恒程知识产权代理事务所 44287
专利代理师 胡海国 魏兰
(51)Int.Cl.
*G06N 20/00*(2019.01)
*G06F 21/60*(2013.01)
(56)对比文件
CN 109284313 A,2019.01.29
CN 107133805 A,2017.09.05
审查员 李华芳

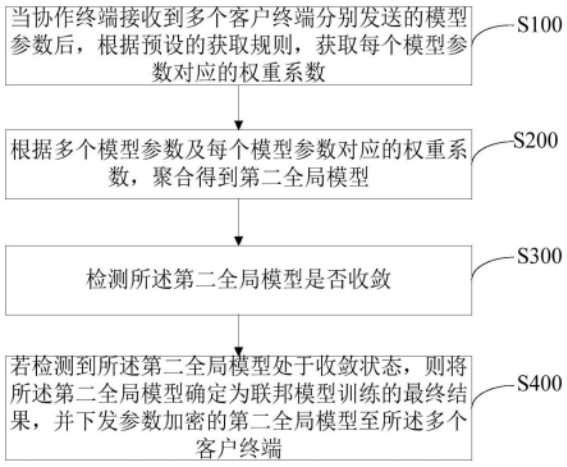
权利要求书3页 说明书13页 附图4页

(54)发明名称

# 联邦模型训练方法、系统、设备及计算机可读存储介质

(57)摘要

本发明公开了一种联邦模型训练方法、系统、设备及计算机可读存储介质，该方法包括步骤：当协作终端接收到多个客户终端分别发送的模型参数后，根据预设的获取规则，获取每个模型参数对应的权重系数；根据多个模型参数及每个模型参数对应的权重系数，聚合得到第二全局模型；检测第二全局模型是否收敛；若检测到第二全局模型处于收敛状态，则将第二全局模型确定为联邦模型训练的最终结果，并下发参数加密的第二全局模型至多个客户终端。本发明实现了协作终端根据每个客户终端的模型参数及其权重系数来更新得到新的全局模型，提升了联邦模型的预测效果。




CN 109871702 B

1.一种联邦模型训练方法,其特征在于,所述联邦模型训练方法包括以下步骤:

当协作终端接收到多个客户终端分别发送的模型参数后,根据预设的获取规则,获取每个模型参数对应的权重系数;其中,所述模型参数是客户终端根据协作终端下发的参数加密的第一全局模型进行联邦模型训练得到的,所述权重系数是基于所述模型参数对应的预测模型的预测准确性确定的;其中,当协作终端接收到多个客户终端分别发送的模型参数后,根据预设的获取规则,获取每个模型参数对应的权重系数的步骤包括:当协作终端接收到多个客户终端分别发送的模型参数后,根据预设的测试样本集,测试并得到每个模型参数对应的预测模型的预测误差率;基于每个预测模型的所述预测误差率及预设的计算公式,分别计算得到每个模型参数对应的权重系数,其中,每个模型参数对应的预测模型的预测误差率与所述模型参数的权重系数负相关;

根据多个模型参数及每个模型参数对应的权重系数,聚合得到第二全局模型;其中,根据多个模型参数及每个模型参数对应的权重系数,聚合得到第二全局模型的步骤包括:分别将每个模型参数与其对应的权重系数相乘,得到多个相乘后的结果;将所述多个相乘后的结果相加,并将相加结果确定为第二全局模型的模型参数,得到所述第二全局模型;

检测所述第二全局模型是否收敛;

若检测到所述第二全局模型处于收敛状态,则将所述第二全局模型确定为联邦模型训练的最终结果,并下发参数加密的第二全局模型至所述多个客户终端。

2.如权利要求1所述的联邦模型训练方法,其特征在于,所述当协作终端接收到多个客户终端分别发送的模型参数后,根据预设的测试样本集,测试并得到每个模型参数对应的预测模型的预测误差率的步骤包括:

当协作终端接收到多个客户终端分别发送的模型参数后,将预设的测试样本集中的多个测试样本输入至所述模型参数对应的预测模型中进行预测,得到所述预测模型针对每个所述测试样本的预测值;

根据多个所述预测值,获取所述测试样本集中预测结果错误的测试样本的数量;

将所述预测结果错误的测试样本的数量与所述测试样本集中全部测试样本数量的比值确定为所述预测模型的预测误差率。

3.如权利要求1-2中任一项所述的联邦模型训练方法,其特征在于,所述当协作终端接收到多个客户终端分别发送的模型参数后,根据预设的获取规则,获取每个模型参数对应的权重系数的步骤之前还包括:

发送参数加密的第一全局模型分别至多个客户终端;

接收所述多个客户终端分别发送的模型参数;

其中,所述客户终端在接收到协作终端下发的所述第一全局模型后,所述客户终端根据所述第一全局模型对第一训练样本集进行预测以得到预测值,并根据所述预测值对所述第一训练样本集进行采样得到第二训练样本集,所述客户终端基于所述第二训练样本集训练所述第一全局模型,训练后得到所述模型参数。

4.如权利要求1所述的联邦模型训练方法,其特征在于,所述检测所述第二全局模型是否收敛的步骤之后还包括:

若检测到所述第二全局模型处于未收敛状态,则下发参数加密的第二全局模型分别至多个客户终端,以使所述多个客户终端分别根据协作终端下发的所述第二全局模型继续迭

代训练以返回模型参数至所述协作终端。

5.如权利要求1所述的联邦模型训练方法,其特征在于,所述当协作终端接收到多个客户终端分别发送的模型参数后,根据预设的获取规则,获取每个模型参数对应的权重系数的步骤之前还包括:

接收多个客户终端分别发送的模型参数;

所述当协作终端接收到多个客户终端分别发送的模型参数后,根据预设的获取规则,获取每个模型参数对应的权重系数的步骤包括:

接收所述多个客户终端分别发送的与所述模型参数对应的权重系数;其中,所述多个客户终端分别根据预设的测试样本集,测试并得到所述模型参数对应的预测模型的预测误差率,并根据所述预测误差率及预设的计算公式,计算得到所述模型参数对应的权重系数。

6.一种联邦模型训练系统,其特征在于,所述系统包括协作终端及分别与所述协作终端通信连接的多个客户终端,所述协作终端包括:

获取模块,用于在接收到多个客户终端分别发送的模型参数后,根据预设的获取规则,获取每个模型参数对应的权重系数;其中,所述模型参数是客户终端根据协作终端下发的参数加密的第一全局模型进行联邦模型训练得到的,所述权重系数是基于所述模型参数对应的预测模型的预测准确性确定的;

聚合更新模块,用于根据多个模型参数及每个模型参数对应的权重系数,聚合得到第二全局模型;其中,所述聚合更新模块包括:乘处理单元,用于分别将每个模型参数与其对应的权重系数相乘,得到多个相乘后的结果;更新单元,用于将所述多个相乘后的结果相加,并将相加结果确定为第二全局模型的模型参数,得到所述第二全局模型;

检测模块,用于检测所述第二全局模型是否收敛;

确定模块,用于在所述检测模块检测到所述第二全局模型处于收敛状态,则将所述第二全局模型确定为联邦模型训练的最终结果,并下发参数加密的第二全局模型至所述多个客户终端;其中,所述获取模块包括:

测试单元,用于在接收到多个客户终端分别发送的模型参数后,根据预设的测试样本集,测试并得到每个模型参数对应的预测模型的预测误差率;

计算单元,用于基于每个预测模型的所述预测误差率及预设的计算公式,分别计算得到每个模型参数对应的权重系数,其中,每个模型参数对应的预测模型的预测误差率与所述模型参数的权重系数负相关。

7.如权利要求6所述的联邦模型训练系统,其特征在于,所述测试单元包括:

测试子单元,用于在接收到多个客户终端分别发送的模型参数后,将预设的测试样本集中的多个测试样本输入至所述模型参数对应的预测模型中进行预测,得到所述预测模型针对每个所述测试样本的预测值;

获取子单元,用于根据多个所述预测值,获取所述测试样本集中预测结果错误的测试样本的数量;

确定子单元,用于将所述预测结果错误的测试样本的数量与所述测试样本集中全部测试样本数量的比值确定为所述预测模型的预测误差率。

8.如权利要求6-7中任一项所述的联邦模型训练系统,其特征在于,所述协作终端还包括:

第一下发模块,用于发送参数加密的第一全局模型分别至多个客户终端;

接收模块,用于接收所述多个客户终端分别发送的模型参数;

其中,所述客户终端在接收到所述第一下发模块下发的所述第一全局模型后,所述客户终端根据所述第一全局模型对第一训练样本集进行预测以得到预测值,并根据所述预测值对所述第一训练样本集进行采样得到第二训练样本集,所述客户终端基于所述第二训练样本集训练所述第一全局模型,训练后得到所述模型参数。

9.如权利要求6所述的联邦模型训练系统,其特征在于,所述协作终端还包括:

第二下发模块,用于在所述检测模块检测到所述第二全局模型处于未收敛状态,则下发参数加密的第二全局模型分别至多个客户终端,以使所述多个客户终端分别根据所述第二下发模块下发的所述第二全局模型继续迭代训练以返回模型参数至所述协作终端。

10.如权利要求6所述的联邦模型训练系统,其特征在于,所述获取模块,还用于接收所述多个客户终端分别发送的与所述模型参数对应的权重系数;其中,所述多个客户终端分别根据预设的测试样本集,测试并得到所述模型参数对应的预测模型的预测误差率,并根据所述预测误差率及预设的计算公式,计算得到所述模型参数对应的权重系数。

11.一种联邦模型训练设备,其特征在于,所述联邦模型训练设备包括存储器、处理器和存储在所述存储器上并可在所述处理器上运行的联邦模型训练程序,所述联邦模型训练程序被所述处理器执行时实现如权利要求1至5中任一项所述的联邦模型训练方法的步骤。

12.一种计算机可读存储介质,其特征在于,所述计算机可读存储介质上存储有联邦模型训练程序,所述联邦模型训练程序被处理器执行时实现如权利要求1至5中任一项所述的联邦模型训练方法的步骤。

# 联邦模型训练方法、系统、设备及计算机可读存储介质

## 技术领域

[0001] 本发明涉及机器学习技术领域，尤其涉及一种联邦模型训练方法、系统、设备及计算机可读存储介质。

## 背景技术

[0002] 联邦模型是利用技术算法加密建造的机器学习模型，联邦学习系统中的多个联邦客户端在模型训练时不用给出己方数据，而是根据协作端下发的参数加密的全局模型和客户端本地的数据集来训练本地模型，并返回本地模型参数供协作端聚合更新全局模型，更新后的全局模型重新下发到客户端，循环往复，直到收敛。联邦学习通过加密机制下参数交换的方式保护客户端数据隐私，客户端数据和客户端的本地模型本身不会进行传输，本地数据不会被反猜，联邦模型在较高程度保持数据完整性的同时，保障了数据隐私。

[0003] 目前，协作端根据多个客户端返回的本地模型参数聚合更新全局模型时，只是对多个客户端的模型参数做简单平均，将平均后的模型参数作为新的全局模型参数下发至客户端继续迭代训练，然而，实际训练中，每个客户端由于其训练数据的不同，训练出的本地模型的预测性能也是参差不齐的，现有的简单平均的聚合方法会导致全局模型的效果不理想。

## 发明内容

[0004] 本发明的主要目的在于提供一种联邦模型训练方法、系统、设备及计算机可读存储介质，旨在解决现有的协作端对多个联邦客户端的模型参数采用简单平均的聚合方式来更新全局模型而导致的联邦模型效果不理想的技术问题。

[0005] 为实现上述目的，本发明提供一种联邦模型训练方法，所述联邦模型训练方法包括步骤：

[0006] 当协作终端接收到多个客户终端分别发送的模型参数后，根据预设的获取规则，获取每个模型参数对应的权重系数；其中，所述模型参数是客户终端根据协作终端下发的参数加密的第一全局模型进行联邦模型训练得到的，所述权重系数是基于所述模型参数对应的预测模型的预测准确性确定的；

[0007] 根据多个模型参数及每个模型参数对应的权重系数，聚合得到第二全局模型；

[0008] 检测所述第二全局模型是否收敛；

[0009] 若检测到所述第二全局模型处于收敛状态，则将所述第二全局模型确定为联邦模型训练的最终结果，并下发参数加密的第二全局模型至所述多个客户终端。

[0010] 可选地，所述当协作终端接收到多个客户终端分别发送的模型参数后，根据预设的获取规则，获取每个模型参数对应的权重系数的步骤包括：

[0011] 当协作终端接收到多个客户终端分别发送的模型参数后，根据预设的测试样本集，测试并得到每个模型参数对应的预测模型的预测误差率；

[0012] 基于每个预测模型的所述预测误差率及预设的计算公式，分别计算得到每个模型

参数对应的权重系数。

[0013] 可选地,所述当协作终端接收到多个客户终端分别发送的模型参数后,根据预设的测试样本集,测试并得到每个模型参数对应的预测模型的预测误差率的步骤包括:

[0014] 当协作终端接收到多个客户终端分别发送的模型参数后,将预设的测试样本集中的多个测试样本输入至所述模型参数对应的预测模型中进行预测,得到所述预测模型针对每个所述测试样本的预测值;

[0015] 根据多个所述预测值,获取所述测试样本集中预测结果错误的测试样本的数量;

[0016] 将所述预测结果错误的测试样本的数量与所述测试样本集中全部测试样本数量的比值确定为所述预预测模型的预测误差率。

[0017] 可选地,所述根据多个模型参数及每个模型参数对应的权重系数,聚合得到第二全局模型的步骤包括:

[0018] 分别将每个模型参数与其对应的权重系数相乘,得到多个相乘后的结果;

[0019] 将所述多个相乘后的结果相加,并将相加结果确定为第二全局模型的模型参数,得到所述第二全局模型。

[0020] 可选地,所述当协作终端接收到多个客户终端分别发送的模型参数后,根据预设的获取规则,获取每个模型参数对应的权重系数的步骤之前还包括:

[0021] 发送参数加密的第一全局模型分别至多个客户终端;

[0022] 接收所述多个客户终端分别发送的模型参数;

[0023] 其中,所述客户终端在接收到协作终端下发的所述第一全局模型后,所述客户终端根据所述第一全局模型对第一训练样本集进行预测以得到预测值,并根据所述预测值对所述第一训练样本集进行采样得到第二训练样本集,所述客户终端基于所述第二训练样本集训练所述第一全局模型,训练后得到所述模型参数。

[0024] 可选地,所述检测所述第二全局模型是否收敛的步骤之后还包括:

[0025] 若检测到所述第二全局模型处于未收敛状态,则下发参数加密的第二全局模型分别至多个客户终端,以使所述多个客户终端分别根据协作终端下发的所述第二全局模型继续迭代训练以返回模型参数至所述协作终端。

[0026] 可选地,所述当协作终端接收到多个客户终端分别发送的模型参数后,根据预设的获取规则,获取每个模型参数对应的权重系数的步骤之前还包括:

[0027] 接收多个客户终端分别发送的模型参数;

[0028] 当协作终端接收到多个客户终端分别发送的模型参数后,根据预设的获取规则,获取每个模型参数对应的权重系数的步骤包括:

[0029] 接收所述多个客户终端分别发送的与所述模型参数对应的权重系数;其中,所述多个客户终端分别根据预设的测试样本集,测试并得到所述模型参数对应的预测模型的预测误差率,并根据所述预测误差率及预设的计算公式,计算得到所述模型参数对应的权重系数。

[0030] 此外,本发明还提出一种联邦模型训练系统,所述系统包括协作终端及分别与所述协作终端通信连接的多个客户终端,所述协作终端包括:

[0031] 获取模块,用于在接收到多个客户终端分别发送的模型参数后,根据预设的获取规则,获取每个模型参数对应的权重系数;其中,所述模型参数是客户终端根据协作终端下

发的参数加密的第一全局模型进行联邦模型训练得到的,所述权重系数是基于所述模型参数对应的预测模型的预测准确性确定的;

[0032] 聚合更新模块,用于根据多个模型参数及每个模型参数对应的权重系数,聚合得到第二全局模型;

[0033] 检测模块,用于检测所述第二全局模型是否收敛;

[0034] 确定模块,用于在所述检测模块检测到所述第二全局模型处于收敛状态,则将所述第二全局模型确定为联邦模型训练的最终结果,并下发参数加密的第二全局模型至所述多个客户终端。

[0035] 可选地,所述获取模块包括:

[0036] 测试单元,用于在接收到多个客户终端分别发送的模型参数后,根据预设的测试样本集,测试并得到每个模型参数对应的预测模型的预测误差率;

[0037] 计算单元,用于基于每个预测模型的所述预测误差率及预设的计算公式,分别计算得到每个模型参数对应的权重系数。

[0038] 可选地,所述测试单元包括:

[0039] 测试子单元,用于在接收到多个客户终端分别发送的模型参数后,将预设的测试样本集中的多个测试样本输入至所述模型参数对应的预测模型中进行预测,得到所述预测模型针对每个所述测试样本的预测值;

[0040] 获取子单元,用于根据多个所述预测值,获取所述测试样本集中预测结果错误的测试样本的数量;

[0041] 确定子单元,用于将所述预测结果错误的测试样本的数量与所述测试样本集中全部测试样本数量的比值确定为所述预预测模型的预测误差率。

[0042] 可选地,所述聚合更新模块包括:

[0043] 乘处理单元,用于分别将每个模型参数与其对应的权重系数相乘,得到多个相乘后的结果;

[0044] 更新单元,用于将所述多个相乘后的结果相加,并将相加结果确定为第二全局模型的模型参数,得到所述第二全局模型。

[0045] 可选地,所述协作终端还包括:

[0046] 第一下发模块,用于发送参数加密的第一全局模型分别至多个客户终端;

[0047] 接收模块,用于接收所述多个客户终端分别发送的模型参数;

[0048] 其中,所述客户终端在接收到所述第一下发模块下发的所述第一全局模型后,所述客户终端根据所述第一全局模型对第一训练样本集进行预测以得到预测值,并根据所述预测值对所述第一训练样本集进行采样得到第二训练样本集,所述客户终端基于所述第二训练样本集训练所述第一全局模型,训练后得到所述模型参数。

[0049] 可选地,所述协作终端还包括:

[0050] 第二下发模块,用于在所述检测模块检测到所述第二全局模型处于未收敛状态,则下发参数加密的第二全局模型分别至多个客户终端,以使所述多个客户终端分别根据所述第二下发模块下发的所述第二全局模型继续迭代训练以返回模型参数至所述协作终端。

[0051] 可选地,所述获取模块,还用于接收所述多个客户终端分别发送的与所述模型参数对应的权重系数;其中,所述多个客户终端分别根据预设的测试样本集,测试并得到所述

模型参数对应的预测模型的预测误差率,并根据所述预测误差率及预设的计算公式,计算得到所述模型参数对应的权重系数。

[0052] 此外,为实现上述目的,本发明还提出一种联邦模型训练设备,所述联邦模型训练设备包括存储器、处理器和存储在所述存储器上并可在所述处理器上运行的联邦模型训练程序,所述联邦模型训练程序被所述处理器执行时实现如上所述的联邦模型训练方法的步骤。

[0053] 此外,为实现上述目的,本发明还提出一种计算机可读存储介质,所述计算机可读存储介质上存储有联邦模型训练程序,所述联邦模型训练程序被处理器执行时实现如上所述的联邦模型训练方法的步骤。

[0054] 本发明通过当协作终端接收到多个客户终端分别发送的模型参数后,根据预设的获取规则,获取每个模型参数对应的权重系数;其中,所述模型参数是客户终端根据协作终端下发的参数加密的第一全局模型进行联邦模型训练得到的,所述权重系数是基于所述模型参数对应的预测模型的预测准确性确定的;根据多个模型参数及每个模型参数对应的权重系数,聚合得到第二全局模型;检测所述第二全局模型是否收敛;若检测到所述第二全局模型处于收敛状态,则将所述第二全局模型确定为联邦模型训练的最终结果,并下发参数加密的第二全局模型至所述多个客户终端;由此,协作终端根据联邦多方的客户端返回的模型参数聚合全局模型时,不是对多个模型参数做简单平均,而是结合每个模型参数的权重系数来更新得到新的全局模型,该权重系数是根据每个客户终端训练模型的预测准确性确定的,提升了联邦模型的预测效果,避免了现有的协作端对多个联邦客户端的模型参数采用简单平均的聚合方式来更新全局模型而导致的联邦模型效果不理想问题。

## 附图说明

[0055] 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;

[0056] 图2为本发明联邦模型训练方法第一实施例的流程示意图;

[0057] 图3为本发明联邦模型训练方法第二实施例的流程示意图;

[0058] 图4为本发明联邦模型训练方法第三实施例的流程示意图;

[0059] 图5为本发明联邦模型训练方法第四实施例的流程示意图。

[0060] 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

[0061] 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。

[0062] 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结构示意图。

[0063] 需要说明的是,图1即可为联邦模型训练设备的硬件运行环境的结构示意图。本发明实施例联邦模型训练设备可以是PC,便携计算机等终端设备。

[0064] 如图1所示,该联邦模型训练设备可以包括: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。

[0065] 本领域技术人员可以理解,图1中示出的联邦模型训练设备结构并不构成对联邦模型训练设备的限定,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。

[0066] 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、用户接口模块以及联邦模型训练程序。其中,操作系统是管理和控制联邦模型训练设备硬件和软件资源的程序,支持联邦模型训练程序以及其它软件或程序的运行。

[0067] 在图1所示的联邦模型训练设备中,用户接口1003主要用于连接客户终端等,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中存储的联邦模型训练程序,并执行以下操作:

[0068] 当协作终端接收到多个客户终端分别发送的模型参数后,根据预设的获取规则,获取每个模型参数对应的权重系数;其中,所述模型参数是客户终端根据协作终端下发的参数加密的第一全局模型进行联邦模型训练得到的,所述权重系数是基于所述模型参数对应的预测模型的预测准确性确定的;

[0069] 根据多个模型参数及每个模型参数对应的权重系数,聚合得到第二全局模型;

[0070] 检测所述第二全局模型是否收敛;

[0071] 若检测到所述第二全局模型处于收敛状态,则将所述第二全局模型确定为联邦模型训练的最终结果,并下发参数加密的第二全局模型至所述多个客户终端。

[0072] 进一步地,所述当协作终端接收到多个客户终端分别发送的模型参数后,根据预设的获取规则,获取每个模型参数对应的权重系数的步骤包括:

[0073] 当协作终端接收到多个客户终端分别发送的模型参数后,根据预设的测试样本集,测试并得到每个模型参数对应的预测模型的预测误差率;

[0074] 基于每个预测模型的所述预测误差率及预设的计算公式,分别计算得到每个模型参数对应的权重系数。

[0075] 进一步地,所述当协作终端接收到多个客户终端分别发送的模型参数后,根据预设的测试样本集,测试并得到每个模型参数对应的预测模型的预测误差率的步骤包括:

[0076] 当协作终端接收到多个客户终端分别发送的模型参数后,将预设的测试样本集中的多个测试样本输入至所述模型参数对应的预测模型中进行预测,得到所述预测模型针对每个所述测试样本的预测值;

[0077] 根据多个所述预测值,获取所述测试样本集中预测结果错误的测试样本的数量;

[0078] 将所述预测结果错误的测试样本的数量与所述测试样本集中全部测试样本数量的比值确定为所述预预测模型的预测误差率。

[0079] 进一步地,所述根据多个模型参数及每个模型参数对应的权重系数,聚合得到第二全局模型的步骤包括:

[0080] 分别将每个模型参数与其对应的权重系数相乘,得到多个相乘后的结果;

[0081] 将所述多个相乘后的结果相加,并将相加结果确定为第二全局模型的模型参数,得到所述第二全局模型。

[0082] 进一步地,所述当协作终端接收到多个客户终端分别发送的模型参数后,根据预

设的获取规则,获取每个模型参数对应的权重系数的步骤之前,处理器1001还可以用于调用存储器1005中存储的联邦模型训练程序,并执行以下步骤:

[0083] 发送参数加密的第一全局模型分别至多个客户终端;

[0084] 接收所述多个客户终端分别发送的模型参数;

[0085] 其中,所述客户终端在接收到协作终端下发的所述第一全局模型后,所述客户终端根据所述第一全局模型对第一训练样本集进行预测以得到预测值,并根据所述预测值对所述第一训练样本集进行采样得到第二训练样本集,所述客户终端基于所述第二训练样本集训练所述第一全局模型,训练后得到所述模型参数。

[0086] 进一步地,所述检测所述第二全局模型是否收敛的步骤之后,处理器1001还可以用于调用存储器1005中存储的联邦模型训练程序,并执行以下步骤:

[0087] 若检测到所述第二全局模型处于未收敛状态,则下发参数加密的第二全局模型分别至多个客户终端,以使所述多个客户终端分别根据协作终端下发的所述第二全局模型继续迭代训练以返回模型参数至所述协作终端。

[0088] 进一步地,所述当协作终端接收到多个客户终端分别发送的模型参数后,根据预设的获取规则,获取每个模型参数对应的权重系数的步骤之前,处理器1001还可以用于调用存储器1005中存储的联邦模型训练程序,并执行以下步骤:

[0089] 接收多个客户终端分别发送的模型参数;

[0090] 当协作终端接收到多个客户终端分别发送的模型参数后,根据预设的获取规则,获取每个模型参数对应的权重系数的步骤包括:

[0091] 接收所述多个客户终端分别发送的与所述模型参数对应的权重系数;其中,所述多个客户终端分别根据预设的测试样本集,测试并得到所述模型参数对应的预测模型的预测误差率,并根据所述预测误差率及预设的计算公式,计算得到所述模型参数对应的权重系数。

[0092] 基于上述的结构,提出联邦模型训练方法的各个实施例。

[0093] 参照图2,图2为本发明联邦模型训练方法第一实施例的流程示意图。

[0094] 本发明实施例提供了联邦模型训练方法的实施例,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。

[0095] 联邦模型训练方法包括:

[0096] 步骤S100,当协作终端接收到多个客户终端分别发送的模型参数后,根据预设的获取规则,获取每个模型参数对应的权重系数;

[0097] 其中,所述模型参数是客户终端根据协作终端下发的参数加密的第一全局模型进行联邦模型训练得到的,所述权重系数是基于所述模型参数对应的预测模型的预测准确性确定的。

[0098] 联邦模型是利用技术算法加密建造的机器学习模型,联邦学习系统为了保证联邦多方客户端在训练过程中数据的保密性,借助第三方协作终端进行加密训练,联邦学习系统中的多个联邦客户端在模型训练时不用给出己方数据,而是根据协作端下发的参数加密的全局模型和客户端本地的数据集来训练本地模型,并返回本地模型参数供协作端聚合更新全局模型,更新后的全局模型重新下发到客户端,循环往复,直到收敛。联邦学习通过加

密机制下参数交换的方式保护客户端数据隐私,客户端数据和客户端的本地模型本身不会进行传输,本地数据不会被反猜,能够在较高程度保持数据完整性的同时,保障数据隐私。

[0099] 但是,现有的协作端根据多个客户端返回的本地模型参数聚合更新全局模型时,只是对多个客户端的模型参数做简单平均,将平均后的模型参数作为新的全局模型参数下发至客户端继续迭代训练,然而,实际训练中,每个客户端由于其训练数据的不同,训练出的本地模型的预测性能也是参差不齐的,现有技术中的简单平均的聚合方法会导致全局模型的效果不理想,若联邦学习系统中每个客户终端的本地模型的预测准确率差异较大,多个参数简单平均的聚合会降低其中本地模型的预测准确率高的客户端的模型效果,全局模型即最终得到的联邦模型的效果不理想。

[0100] 本实施例中,协作终端采用预设的加密算法对第一全局模型的参数加密,并下发参数加密的第一全局模型至联邦学习系统中的多个客户终端,其中,预设的加密算法本实施例不做具体限制,可以是非对称加密算法等等,第一全局模型是本实施例待训练联邦模型完成了若干次迭代运算后得到的全局模型。

[0101] 进一步地,客户终端在接收到协作终端下发的参数加密的第一全局模型后,每个客户终端根据其本地的训练样本数据对该第一全局模型进行训练得到其各自的本地模型,需要说明的是,本实施例中,多个客户端的训练样本类别均服从独立同分布,客户终端将得到的本地模型的模型参数返回至协作终端。

[0102] 当协作终端接收到多个客户终端分别发送的模型参数后,根据预设的获取规则,获取每个模型参数对应的权重系数,所述权重系数是基于所述模型参数对应的预测模型的预测准确性确定的,作为一种实施方式,协作终端存储有测试样本集,测试样本集中的测试样本与多个客户终端的训练样本均具有相同的特征维度,在接收到多个客户终端分别发送的模型参数后,协作终端采用测试样本集,测试每个模型参数对应的预测模型的预测准确性,具体地,将测试样本集中的多个测试样本输入至每个客户终端回传的预测模型中,得到该预测模型对该测试样本集中多个测试样本的预测结果,筛选出预测错误的测试样本的数量,用筛选出的预测错误的测试样本的数量除该测试样本集中测试样本的总数,即得到当前预测模型的预测误差率,采用同样的方法,得到每个客户终端发送的模型参数对应的预测模型的预测误差率。

[0103] 进一步地,根据每个模型参数下的预测误差率确定该模型参数参与全局模型聚合时的权重系数,每个模型参数下的预测误差率与该模型参数的权重系数负相关,即模型参数对应的预测模型的预测误差率越小,则该模型参数的权重系数越大,本实施例协作终端根据多个客户终端发送的模型参数聚合时,对预测准确性高的模型增加其模型参数的权重,对预测准确性低的模型降低其模型参数的权重,以此更新得到的新的全局模型保证了每个客户终端模型效果的增长。作为一种实施方式,权重系数的计算可以是根据计算公式 $\alpha_i = \frac{1}{2}\ln\left(\frac{1-\varepsilon_i}{\varepsilon_i}\right)$ 计算得到,其中,$\varepsilon_i$为第i个客户终端的预测模型的预测误差率,$\alpha_i$为第i个客户终端的预测模型的模型参数对应的权重系数,i为大于零的整数,协作终端即获取到每个模型参数对应的权重系数。

[0104] 需要说明的是,在其它实施例中,联邦学习系统中的多个客户终端可以均存储有相同的测试样本集,该测试样本集中的测试样本与多个客户终端的训练样本均具有相同的

特征维度,每个客户终端的模型参数对应的权重系数可以是客户终端根据本地存储的测试样本集测试其预测模型的预测误差率,进而得到其模型参数对应的权重系数,客户终端发送模型参数的同时,将计算得到的模型参数对应的权重系数也一并发至协作终端供协作终端聚合,本实施例在此不做具体限制,进一步地,权重系数的计算方法也不限于本实施例所述的计算方法,在其它实施例中,可以根据需求设置相应的计算规则。

[0105] 步骤S200,根据多个模型参数及每个模型参数对应的权重系数,聚合得到第二全局模型;

[0106] 本实施例中,每个模型参数对应的预测模型的预测误差率与该模型参数的权重系数负相关,即预测误差率越小则该模型参数的权重系数越大,预测误差率越大则该模型参数的权重系数越小,对每个模型参数乘其对应的权重系数,再将乘了权重系数的多个模型参数相加即得到新的全局模型的参数,得到新的全局模型即第二全局模型。

[0107] 本实施例协作终端根据多个客户终端发送的模型参数聚合时,对预测准确性高的模型增加其模型参数的权重,对预测准确性低的模型降低其模型参数的权重,以此更新得到的新的全局模型保证了每个客户终端模型效果的增长,避免了现有的协作端对多个联邦客户端的模型参数采用简单平均的聚合方式来更新全局模型而导致的联邦模型效果不理想问题。

[0108] 步骤S300,检测所述第二全局模型是否收敛;

[0109] 本实施例中,作为一种实施方式,协作终端根据第二全局模型的损失函数得到损失值,根据损失值判断第二全局模型是否收敛,具体地,协作终端存储有第一全局模型下的第一损失值,协作终端根据第二全局模型的损失函数得到第二损失值,计算第一损失值和第二损失值之间的差值,并判断该差值是否小于或者等于预设阈值,若该差值小于或者等于预设阈值,则确定所述第二全局模型处于收敛状态,联邦模型训练完成,实际训练时,预设阈值可以根据用户的需求来自行设定,本实施例对预设阈值不做具体限制。

[0110] 步骤S400,若检测到所述第二全局模型处于收敛状态,则将所述第二全局模型确定为联邦模型训练的最终结果,并下发参数加密的第二全局模型至所述多个客户终端。

[0111] 若检测到第二全局模型处于收敛状态,则联邦模型训练完成,第二全局模型即确定为联邦模型训练的最终结果,协作终端下发参数加密的第二全局模型至所述多个客户终端,多个客户终端即在不用给出己方数据的前提下,实现了本地模型的效果增长,保障数据隐私的同时,提升了预测准确性。

[0112] 本实施例通过当协作终端接收到多个客户终端分别发送的模型参数后,根据预设的获取规则,获取每个模型参数对应的权重系数;其中,所述模型参数是客户终端根据协作终端下发的参数加密的第一全局模型进行联邦模型训练得到的,所述权重系数是基于所述模型参数对应的预测模型的预测准确性确定的;根据多个模型参数及每个模型参数对应的权重系数,聚合得到第二全局模型;检测所述第二全局模型是否收敛;若检测到所述第二全局模型处于收敛状态,则将所述第二全局模型确定为联邦模型训练的最终结果,并下发参数加密的第二全局模型至所述多个客户终端;由此,协作终端根据联邦多方的客户端返回的模型参数聚合全局模型时,不是对多个模型参数做简单平均,而是结合每个模型参数的权重系数来更新得到新的全局模型,该权重系数是根据每个客户终端训练模型的预测准确性确定的,提升了联邦模型的预测效果,避免了现有的协作端对多个联邦客户端的模型参

数采用简单平均的聚合方式来更新全局模型而导致的联邦模型效果不理想问题。

[0113] 进一步地,提出本发明联邦模型训练方法第二实施例。

[0114] 参照图3,图3为本发明联邦模型训练方法第二实施例的流程示意图,基于上述图2所示的实施例,本实施例中,步骤S100,当协作终端接收到多个客户终端分别发送的模型参数后,根据预设的获取规则,获取每个模型参数对应的权重系数的步骤包括:

[0115] 步骤S101,当协作终端接收到多个客户终端分别发送的模型参数后,根据预设的测试样本集,测试并得到每个模型参数对应的预测模型的预测误差率;

[0116] 步骤S102,基于每个预测模型的所述预测误差率及预设的计算公式,分别计算得到每个模型参数对应的权重系数。

[0117] 具体地,在本实施例中,协作终端存储有测试样本集,测试样本集中包括多个测试样本,多个测试样本与多个客户终端的本地训练样本均具有相同的特征维度,协作终端将测试样本集中的多个测试样本输入至每个客户终端回传的预测模型中,得到该预测模型对该测试样本集中多个测试样本的预测结果,筛选得到预测结果错误的测试样本的数量,用预测结果错误的测试样本的数量除该测试样本集中测试样本的总数,即得到当前预测模型的预测误差率,进一步地,采用同样的方法,得到每个客户终端发送的模型参数对应的预测模型的预测误差率。

[0118] 在本实施例中,预设的计算公式为:$\alpha_i = \frac{1}{2}\ln\left(\frac{1-\varepsilon_i}{\varepsilon_i}\right)$,其中,$\varepsilon_i$为第i个客户终端的预测模型的预测误差率,$\alpha_i$为第i个客户终端的预测模型的模型参数对应的权重系数,i为大于零的整数;协作终端通过计算得到每个客户终端的预测模型的预测误差率后,分别将每个预测误差率代入该计算公式计算,得到的结果即为每个模型参数对应的权重系数。

[0119] 进一步地,基于上述图2所示的实施例,本实施例中,步骤S200,根据多个模型参数及每个模型参数对应的权重系数,聚合得到第二全局模型的步骤包括:

[0120] 步骤S201,分别将每个模型参数与其对应的权重系数相乘,得到多个相乘后的结果;

[0121] 步骤S202,将所述多个相乘后的结果相加,并将相加结果确定为第二全局模型的模型参数,得到所述第二全局模型。

[0122] 本实施例中,对每个模型参数乘其对应的权重系数,再将乘了权重系数的多个模型参数相加即得到新的全局模型的参数,得到新的全局模型即第二全局模型。

[0123] 本实施例协作终端根据多个客户终端发送的模型参数聚合时,对预测准确性高的模型增加其模型参数的权重,对预测准确性低的模型降低其模型参数的权重,以此更新得到的新的全局模型保证了每个客户终端模型效果的增长,避免了现有的协作端对多个联邦客户端的模型参数采用简单平均的聚合方式来更新全局模型而导致的联邦模型效果不理想问题。

[0124] 进一步地,提出本发明联邦模型训练方法第三实施例。

[0125] 参照图4,图4为本发明联邦模型训练方法第三实施例的流程示意图,基于上述图2所示的实施例,本实施例中,步骤S100,当协作终端接收到多个客户终端分别发送的模型参数后,根据预设的获取规则,获取每个模型参数对应的权重系数的步骤之前还包括:

[0126] 步骤S110,发送参数加密的第一全局模型分别至多个客户终端;

[0127] 步骤S120,接收所述多个客户终端分别发送的模型参数;

[0128] 其中,所述客户终端在接收到协作终端下发的所述第一全局模型后,所述客户终端根据所述第一全局模型对第一训练样本集进行预测以得到预测值,并根据所述预测值对所述第一训练样本集进行采样得到第二训练样本集,所述客户终端基于所述第二训练样本集训练所述第一全局模型,训练后得到所述模型参数。

[0129] 本实施例中,作为一种实施方式,假设待训练的联邦模型已经完成了第k次的迭代运算并得到第一全局模型$model_k$,其中,k为大于零的整数,本实施例联邦模型训练方法具体包括如下步骤;

[0130] 步骤a:协作终端发送参数加密的第一全局模型$model_k$分别至每一个联邦客户终端;

[0131] 步骤b:第i个客户终端接收$model_k$,用$model_k$对本地的训练样本集$X_i$进行预测,根据预测结果将$X_i$中的训练样本分为两个集合:预测错误的样本数据集$(x_1,x_2,...,x_n)$和预测正确的样本数据集$(y_1,y_2,...,y_m)$,其中n表示$X_i$中预测错误的样本数量,m表示$X_i$中预测正确的样本数量,n可以等于m,本实施例不做具体限制,故有:

[0132] $X_i=(x_1,x_2,...,x_n)\cup(y_1,y_2,...,y_m)$ 且$(x_1,x_2,...,x_n)\cap(y_1,y_2,...,y_m)=\varnothing$ 成立;

[0133] 第i个客户终端在训练$model_k$之前,先对$X_i$进行采样,具体是选取所述预测错误的样本数据集$(x_1,x_2,...,x_n)$,并从所述预测正确的样本数据集$(y_1,y_2,...,y_m)$中抽取部分样本$(y_1,y_2,...,y_k)$,$k<m$,来构成采样后的训练数据集$Y_i$,即$Y_i=(x_1,x_2,...,x_n)\cup(y_1,y_2,...,y_k)$,$k<n$,采用训练数据集$Y_i$对$model_k$进行训练,训练后得到新的本地预测模型$mod\,el_{k+1}^i$。

[0134] 步骤c:第i个客户终端发送训练后得到的本地预测模型至协作终端,协作终端将协作终端存储的测试样本集中的多个测试样本输入至第i个客户终端回传的预测模型中,得到该预测模型对该测试样本集中多个测试样本的预测结果,筛选出预测错误的测试样本的数量,用筛选出的预测错误的测试样本的数量除该测试样本集中测试样本的总数,即得到第i个客户终端的预测模型的预测误差率$\varepsilon_{k+1}^i$;

[0135] 步骤d:协作终端将计算得到的第i个客户终端的预测模型的预测误差率$\varepsilon_{k+1}^i$代入计算公式$\alpha_{k+1}^i=\frac{1}{2}\ln\left(\frac{1-\varepsilon_{k+1}^i}{\varepsilon_{k+1}^i}\right)$中,计算得到第i个客户终端的模型参数对应的权重系数$\alpha_{k+1}^i$。

[0136] 步骤e:协作终端根据每一个客户终端发送的模型参数及计算得到的每一个模型参数对应的权重系数,聚合更新第一全局模型$model_k$得到第二全局模型$model_{k+1}$,其中$mod\,el_{k+1}=\sum_{i=1}^{q}\left(mod\,el_{k+1}^i*\alpha_{k+1}^i\right)$,q为本实施例联邦客户终端的总数量,协作终端检测$model_{k+1}$是否收敛,若收敛,则将$model_{k+1}$作为本实施例联邦模型的最终训练结果,并将$model_{k+1}$的模型参数加密下发至各个客户终端。

[0137] 若协作终端检测到$model_{k+1}$未收敛,则重复上述步骤a-步骤e,直至联邦模型收敛。

[0138] 本实施例客户终端根据协作终端下发的参数加密的第一全局模型训练时,客户终端首先根据所述第一全局模型对客户终端的本地第一训练样本集进行预测以得到预测值,

并根据所述预测值对所述第一训练样本集进行采样得到第二训练样本集,所述客户终端基于所述第二训练样本集训练所述第一全局模型,训练后得到所述模型参数并回传所述模型参数至协作终端,实现了对于预测错误的样本数据,在下一次迭代时提高其权重,优化了本地训练模型的性能即提升了每个客户终端发送至协作终端的模型参数的质量,从而提升了全局模型即本实施例联邦模型的预测准确性。

[0139] 进一步地,提出本发明联邦模型训练方法第四实施例。

[0140] 参照图5,图5为本发明联邦模型训练方法第四实施例的流程示意图,基于图2所示的实施例,本实施例中,步骤S300,检测所述第二全局模型是否收敛的步骤之后还包括:

[0141] 步骤S500,若检测到所述第二全局模型处于未收敛状态,则下发参数加密的第二全局模型分别至多个客户终端,以使所述多个客户终端分别根据协作终端下发的所述第二全局模型继续迭代训练以返回模型参数至所述协作终端。

[0142] 本实施例中,若检测到所述第二全局模型处于未收敛状态,则下发参数加密的第二全局模型分别至多个客户终端,当协作终端接收到多个客户终端分别发送的模型参数后,根据预设的获取规则,获取每个模型参数对应的权重系数;其中,所述模型参数是客户终端根据协作终端下发的参数加密的第二全局模型进行联邦模型训练得到的,所述权重系数是基于所述模型参数对应的预测模型的预测准确性确定的;根据多个模型参数及每个模型参数对应的权重系数,聚合得到第三全局模型;检测所述第三全局模型是否收敛;若检测到所述第三全局模型处于收敛状态,则将所述第三全局模型确定为联邦模型训练的最终结果,并下发参数加密的第三全局模型至所述多个客户终端,若检测到所述第三全局模型处于未收敛状态,下发参数加密的第三全局模型分别至多个客户终端,重复本发明上述任一实施例的步骤,继续训练直至模型收敛。

[0143] 进一步地,提出本发明联邦模型训练方法第五实施例。

[0144] 基于图2所示的实施例,本实施例中,步骤S100,当协作终端接收到多个客户终端分别发送的模型参数后,根据预设的获取规则,获取每个模型参数对应的权重系数的步骤之前还包括步骤:

[0145] 接收多个客户终端分别发送的模型参数;

[0146] 步骤S100,当协作终端接收到多个客户终端分别发送的模型参数后,根据预设的获取规则,获取每个模型参数对应的权重系数的步骤包括:

[0147] 接收所述多个客户终端分别发送的与所述模型参数对应的权重系数;其中,所述多个客户终端分别根据预设的测试样本集,测试并得到所述模型参数对应的预测模型的预测误差率,并根据所述预测误差率及预设的计算公式,计算得到所述模型参数对应的权重系数。

[0148] 本实施例中,作为一种实施方式,每个客户终端的模型参数对应的权重系数的计算是在各个客户终端分别进行的,联邦学习系统中的多个客户终端均存储有相同的测试样本集,该测试样本集中的测试样本与多个客户终端的训练样本均具有相同的特征维度,每个客户终端的模型参数对应的权重系数可以是客户终端根据本地存储的测试样本集测试其预测模型的预测误差率,进而得到其模型参数对应的权重系数,客户终端发送模型参数的同时,将计算得到的模型参数对应的权重系数也一并发至协作终端供协作终端聚合得到全局模型。

[0149] 此外,本发明实施例还提出一种联邦模型训练系统,所述系统包括协作终端及分别与所述协作终端通信连接的多个客户终端,所述协作终端包括:

[0150] 获取模块,用于在接收到多个客户终端分别发送的模型参数后,根据预设的获取规则,获取每个模型参数对应的权重系数;其中,所述模型参数是客户终端根据协作终端下发的参数加密的第一全局模型进行联邦模型训练得到的,所述权重系数是基于所述模型参数对应的预测模型的预测准确性确定的;

[0151] 聚合更新模块,用于根据多个模型参数及每个模型参数对应的权重系数,聚合得到第二全局模型;

[0152] 检测模块,用于检测所述第二全局模型是否收敛;

[0153] 确定模块,用于在所述检测模块检测到所述第二全局模型处于收敛状态,则将所述第二全局模型确定为联邦模型训练的最终结果,并下发参数加密的第二全局模型至所述多个客户终端。

[0154] 优选地,所述获取模块包括:

[0155] 测试单元,用于在接收到多个客户终端分别发送的模型参数后,根据预设的测试样本集,测试并得到每个模型参数对应的预测模型的预测误差率;

[0156] 计算单元,用于基于每个预测模型的所述预测误差率及预设的计算公式,分别计算得到每个模型参数对应的权重系数。

[0157] 优选地,所述测试单元包括:

[0158] 测试子单元,用于在接收到多个客户终端分别发送的模型参数后,将预设的测试样本集中的多个测试样本输入至所述模型参数对应的预测模型中进行预测,得到所述预测模型针对每个所述测试样本的预测值;

[0159] 获取子单元,用于根据多个所述预测值,获取所述测试样本集中预测结果错误的测试样本的数量;

[0160] 确定子单元,用于将所述预测结果错误的测试样本的数量与所述测试样本集中全部测试样本数量的比值确定为所述预预测模型的预测误差率。

[0161] 优选地,所述预设的计算公式为:$\alpha_i = \frac{1}{2}\ln\left(\frac{1-\varepsilon_i}{\varepsilon_i}\right)$;其中,$\varepsilon_i$为第i个客户终端的预测模型的预测误差率,$\alpha_i$为第i个客户终端的所述预测模型的模型参数对应的权重系数,i为大于零的整数。

[0162] 优选地,所述聚合更新模块包括:

[0163] 乘处理单元,用于分别将每个模型参数与其对应的权重系数相乘,得到多个相乘后的结果;

[0164] 更新单元,用于将所述多个相乘后的结果相加,并将相加结果确定为第二全局模型的模型参数,得到所述第二全局模型。

[0165] 优选地,所述协作终端还包括:

[0166] 第一下发模块,用于发送参数加密的第一全局模型分别至多个客户终端;

[0167] 接收模块,用于接收所述多个客户终端分别发送的模型参数;

[0168] 其中,所述客户终端在接收到所述第一下发模块下发的所述第一全局模型后,所述客户终端根据所述第一全局模型对第一训练样本集进行预测以得到预测值,并根据所述

预测值对所述第一训练样本集进行采样得到第二训练样本集,所述客户终端基于所述第二训练样本集训练所述第一全局模型,训练后得到所述模型参数。

[0169] 优选地,所述协作终端还包括:

[0170] 第二下发模块,用于在所述检测模块检测到所述第二全局模型处于未收敛状态,则下发参数加密的第二全局模型分别至多个客户终端,以使所述多个客户终端分别根据所述第二下发模块下发的所述第二全局模型继续迭代训练以返回模型参数至所述协作终端。

[0171] 优选地,所述获取模块,还用于接收所述多个客户终端分别发送的与所述模型参数对应的权重系数;其中,所述多个客户终端分别根据预设的测试样本集,测试并得到所述模型参数对应的预测模型的预测误差率,并根据所述预测误差率及预设的计算公式,计算得到所述模型参数对应的权重系数。

[0172] 本发明联邦模型训练系统具体实施方式与上述联邦模型训练方法各实施例基本相同,在此不再赘述。

[0173] 此外,本发明实施例还提出一种计算机可读存储介质,所述计算机可读存储介质上存储有联邦模型训练程序,所述联邦模型训练程序被处理器执行时实现如上所述的奖励发送方法的步骤。

[0174] 本发明计算机可读存储介质具体实施方式与上述联邦模型训练方法各实施例基本相同,在此不再赘述。

[0175] 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。

[0176] 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。

[0177] 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。

[0178] 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。

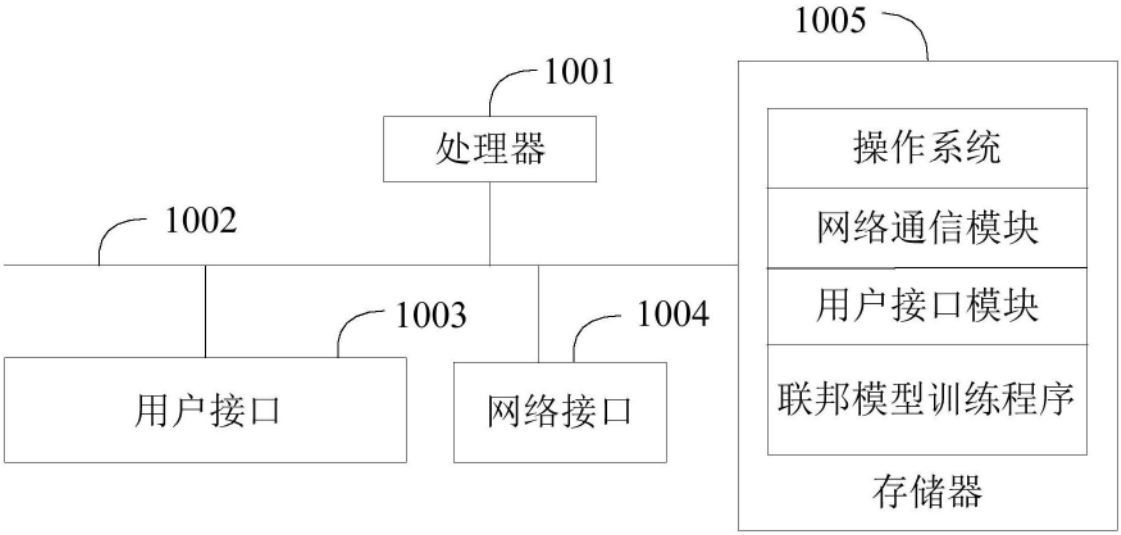

1005
1001
处理器
操作系统
网络通信模块
1002
用户接口模块
1003
1004
用户接口
网络接口
联邦模型训练程序
存储器

图1

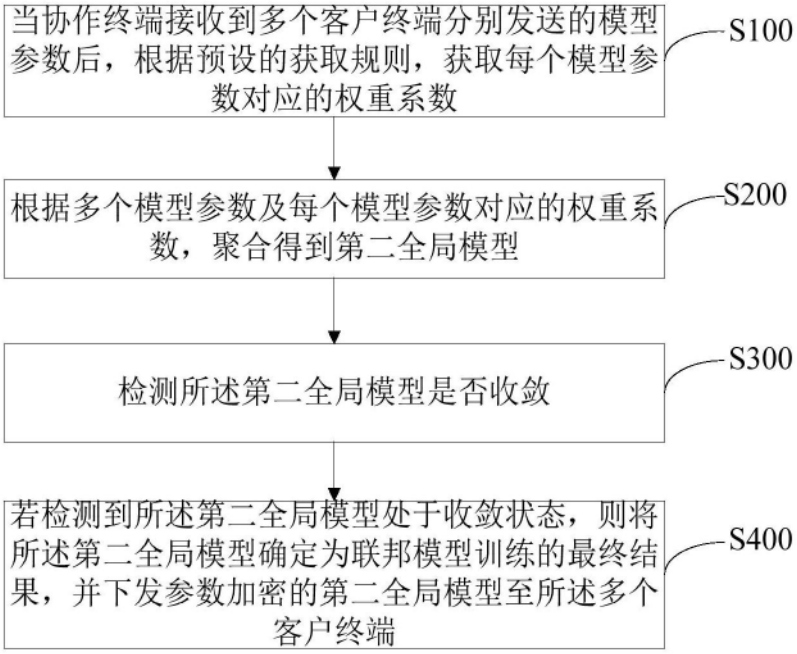

当协作终端接收到多个客户终端分别发送的模型参数后，根据预设的获取规则，获取每个模型参数对应的权重系数
S100
根据多个模型参数及每个模型参数对应的权重系数，聚合得到第二全局模型
S200
检测所述第二全局模型是否收敛
S300
若检测到所述第二全局模型处于收敛状态，则将所述第二全局模型确定为联邦模型训练的最终结果，并下发参数加密的第二全局模型至所述多个客户终端
S400

图2

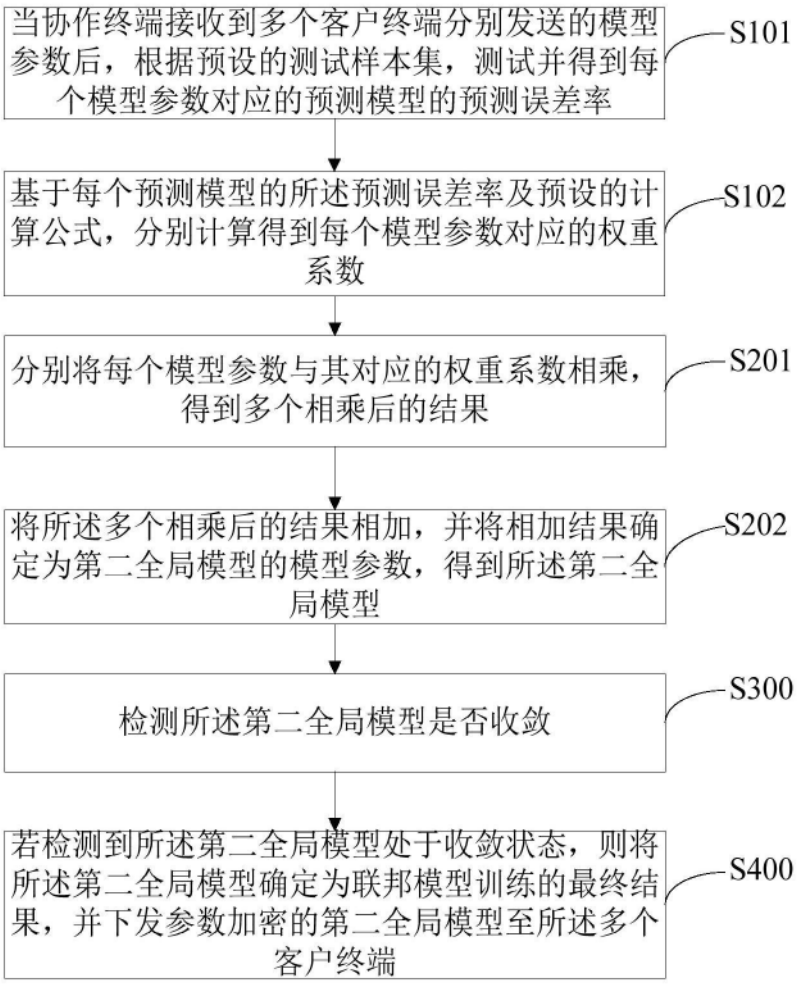

当协作终端接收到多个客户终端分别发送的模型参数后，根据预设的测试样本集，测试并得到每个模型参数对应的预测模型的预测误差率
S101
基于每个预测模型的所述预测误差率及预设的计算公式，分别计算得到每个模型参数对应的权重系数
S102
分别将每个模型参数与其对应的权重系数相乘，得到多个相乘后的结果
S201
将所述多个相乘后的结果相加，并将相加结果确定为第二全局模型的模型参数，得到所述第二全局模型
S202
检测所述第二全局模型是否收敛
S300
若检测到所述第二全局模型处于收敛状态，则将所述第二全局模型确定为联邦模型训练的最终结果，并下发参数加密的第二全局模型至所述多个客户终端
S400

图3

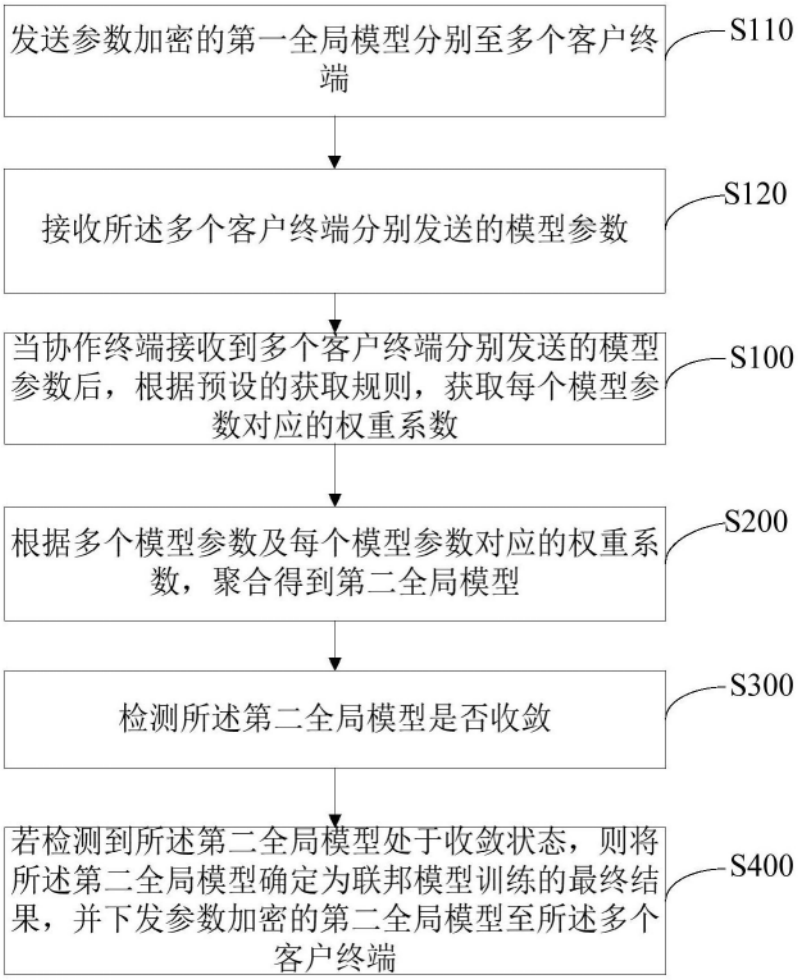

发送参数加密的第一全局模型分别至多个客户终端
S110
接收所述多个客户终端分别发送的模型参数
S120
当协作终端接收到多个客户终端分别发送的模型参数后，根据预设的获取规则，获取每个模型参数对应的权重系数
S100
根据多个模型参数及每个模型参数对应的权重系数，聚合得到第二全局模型
S200
检测所述第二全局模型是否收敛
S300
若检测到所述第二全局模型处于收敛状态，则将所述第二全局模型确定为联邦模型训练的最终结果，并下发参数加密的第二全局模型至所述多个客户终端
S400

图4

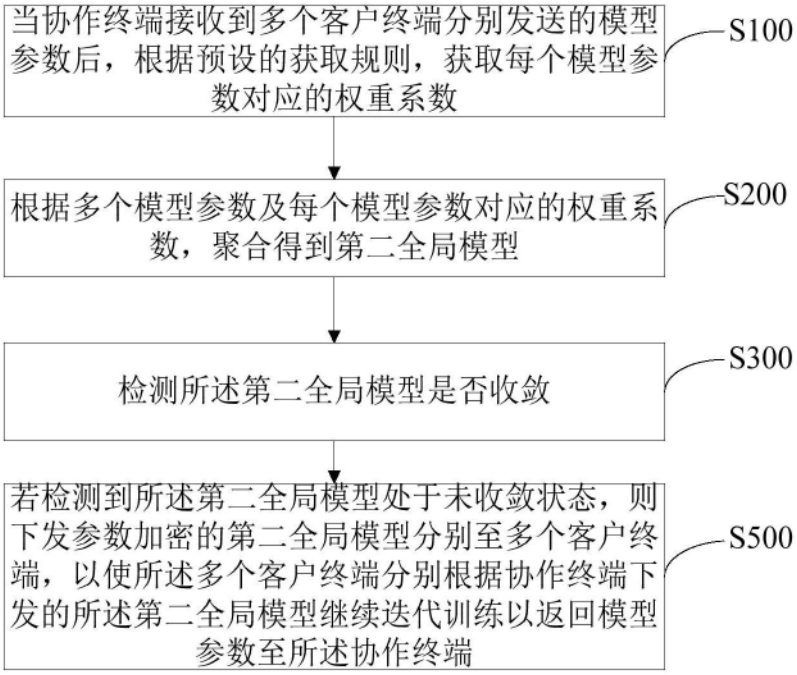

当协作终端接收到多个客户终端分别发送的模型参数后，根据预设的获取规则，获取每个模型参数对应的权重系数
S100
根据多个模型参数及每个模型参数对应的权重系数，聚合得到第二全局模型
S200
检测所述第二全局模型是否收敛
S300
若检测到所述第二全局模型处于未收敛状态，则下发参数加密的第二全局模型分别至多个客户终端，以使所述多个客户终端分别根据协作终端下发的所述第二全局模型继续迭代训练以返回模型参数至所述协作终端
S500

图5