(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 113177645 B
(45)授权公告日 2021.09.28

(21)申请号 202110726072.4
(22)申请日 2021.06.29
(65)同一申请的已公布的文献号
申请公布号 CN 113177645 A
(43)申请公布日 2021.07.27
(73)专利权人 腾讯科技(深圳)有限公司
地址 518057 广东省深圳市南山区高新区科技中一路腾讯大厦35层
(72)发明人 程勇 蒋杰 刘煜宏 陈鹏 陶阳宇
(74)专利代理机构 北京三高永信知识产权代理有限责任公司 11138
代理人 张所明
(51)Int.Cl.
G06N 20/00(2019.01)
(56)对比文件
CN 111008709 A,2020.04.14
CN 111008709 A,2020.04.14
CN 110929885 A,2020.03.27
CN 112631775 A,2021.04.09
CN 110059829 A,2019.07.26
WO 2021059604 A1,2021.04.01
US 2021117624 A1,2021.04.22
CN 111813526 A,2020.10.23
CN 111062044 A,2020.04.24
肖林声 等."基于并行同态加密和 STC 的高效安全联邦学习".《通信技术》.2021,第54卷(第4期),
Senapati Sang Diwangkara 等."Study of Data Imbalance and Asynchronous Aggregation Algorithm on Federated Learning System".《2020 International Conference on Information Technology Systems and Innovation》.2020,
审查员 秦涛

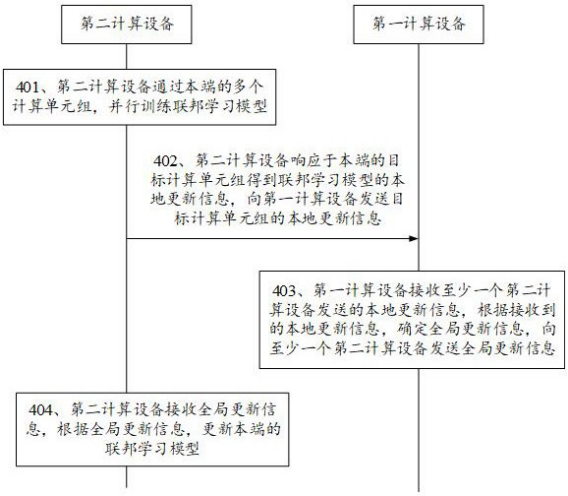
权利要求书4页 说明书22页 附图8页

(54)发明名称

联邦学习方法、装置、计算设备及存储介质

(57)摘要

本申请实施例公开了一种联邦学习方法、装置、计算设备及存储介质，属于计算机技术领域。该方法包括：第二计算设备通过多个计算单元组，并行训练联邦学习模型；第二计算设备响应于目标计算单元组得到联邦学习模型的本地更新信息，向第一计算设备发送本地更新信息；第一计算设备接收至少一个第二计算设备发送的本地更新信息，根据接收到的本地更新信息确定全局更新信息，向至少一个第二计算设备发送全局更新信息；第二计算设备根据全局更新信息更新联邦学习模型。本申请实施例采用基于计算单元组的方式发送本地更新信息，无需等待所有计算单元组，第二计算设备能够及时参与到联邦学习模型的全局训练中，有利于提高联邦学习的效率。



CN 113177645 B

1.一种联邦学习方法,其特征在于,应用于模型训练系统,所述模型训练系统包括第一计算设备和多个第二计算设备,所述方法包括:

在所述第二计算设备包括n个计算单元的情况下,所述第二计算设备将样本数据划分为n个样本数据集合,每个样本数据集合包括至少一个样本数据,所述n为大于1的整数;

所述第二计算设备将所述n个样本数据集合分配给所述n个计算单元;

所述第二计算设备通过本端的多个计算单元组中的每个计算单元,基于所述计算单元分配到的样本数据集合,并行训练联邦学习模型,每个计算单元组包括至少一个计算单元;

所述第二计算设备响应于本端的目标计算单元组得到所述联邦学习模型的本地更新信息,向所述第一计算设备发送所述目标计算单元组的本地更新信息,所述本地更新信息用于更新所述联邦学习模型,所述目标计算单元组为所述多个计算单元组中的任一个计算单元组;

所述第一计算设备接收至少一个第二计算设备发送的本地更新信息,根据接收到的本地更新信息,确定全局更新信息,向至少一个第二计算设备发送所述全局更新信息;

所述第二计算设备接收所述全局更新信息,根据所述全局更新信息,更新本端的联邦学习模型;

其中,所述第二计算设备通过本端的多个计算单元组中的每个计算单元,基于所述计算单元分配到的样本数据集合,并行训练联邦学习模型,包括:

所述第二计算设备在所述n个计算单元中,确定至少一个目标计算单元;

所述第二计算设备将所述目标计算单元分配到的样本数据集合进行拆分,得到多个样本数据组,每个样本数据组包括至少一个样本数据;

所述第二计算设备通过所述目标计算单元,基于所述多个样本数据组中的每个样本数据组,分别对所述联邦学习模型进行迭代训练。

2.根据权利要求1所述的方法,其特征在于,所述第二计算设备响应于本端的目标计算单元组得到所述联邦学习模型的本地更新信息,向所述第一计算设备发送所述目标计算单元组的本地更新信息,包括:

在所述目标计算单元组包括多个计算单元的情况下,所述第二计算设备响应于所述目标计算单元组中的每个计算单元得到所述联邦学习模型的本地更新信息,向所述第一计算设备发送所述目标计算单元组中的每个计算单元的本地更新信息。

3.根据权利要求1所述的方法,其特征在于,所述第二计算设备响应于本端的目标计算单元组得到所述联邦学习模型的本地更新信息,向所述第一计算设备发送所述目标计算单元组的本地更新信息,包括:

在所述目标计算单元组包括多个计算单元的情况下,所述第二计算设备响应于所述目标计算单元组中的每个计算单元得到所述联邦学习模型的本地更新信息,对所述目标计算单元组中的每个计算单元的本地更新信息进行融合,得到融合更新信息;

向所述第一计算设备发送所述融合更新信息。

4.根据权利要求1所述的方法,其特征在于,所述第一计算设备接收至少一个第二计算设备发送的本地更新信息,根据接收到的本地更新信息,确定全局更新信息,向至少一个第二计算设备发送所述全局更新信息,包括:

所述第一计算设备接收目标数量的第二计算设备发送的本地更新信息,根据接收到的

本地更新信息，确定所述全局更新信息；

所述第一计算设备向每个第二计算设备发送所述全局更新信息。

5.根据权利要求1所述的方法，其特征在于，所述第一计算设备接收至少一个第二计算设备发送的本地更新信息，根据接收到的本地更新信息，确定全局更新信息，向至少一个第二计算设备发送所述全局更新信息，包括：

所述第一计算设备接收目标数量的第二计算设备发送的本地更新信息，确定迭代轮次之差，所述迭代轮次之差为各个第二计算设备中最大的已迭代轮次与最小的已迭代轮次之差；

所述第一计算设备在所述迭代轮次之差不大于目标阈值的情况下，根据接收到的本地更新信息，确定所述全局更新信息；

所述第一计算设备向至少一个第二计算设备发送所述全局更新信息。

6.根据权利要求5所述的方法，其特征在于，所述方法还包括：

所述第一计算设备在所述迭代轮次之差大于所述目标阈值的情况下，接收每个第二计算设备发送的每个计算单元的本地更新信息，根据接收到的本地更新信息，确定所述全局更新信息；

所述第一计算设备向所述每个第二计算设备发送所述全局更新信息。

7.根据权利要求1所述的方法，其特征在于，所述第二计算设备响应于本端的目标计算单元组得到所述联邦学习模型的本地更新信息，向所述第一计算设备发送所述目标计算单元组的本地更新信息，包括：

所述第二计算设备响应于本端的目标计算单元组中的每个计算单元得到所述联邦学习模型的本地更新信息，通过所述第二计算设备与所述第一计算设备之间的网络链路，向所述第一计算设备发送所述目标计算单元组的本地更新信息；或者，

所述第二计算设备响应于本端的目标计算单元组中的每个计算单元得到所述联邦学习模型的本地更新信息，通过每个计算单元与所述第一计算设备之间的网络链路，分别向所述第一计算设备发送所述每个计算单元的本地更新信息；或者，

所述第二计算设备响应于本端的目标计算单元组中的每个计算单元得到所述联邦学习模型的本地更新信息，通过所述目标计算单元组与所述第一计算设备之间的网络链路，向所述第一计算设备发送所述目标计算单元组的本地更新信息。

8.根据权利要求1所述的方法，其特征在于，所述第一计算设备接收至少一个第二计算设备发送的本地更新信息，根据接收到的本地更新信息，确定全局更新信息，包括：

所述第一计算设备接收多个第二计算设备发送的本地更新信息，对接收到的多个本地更新信息进行融合，得到所述全局更新信息。

9.一种联邦学习方法，其特征在于，应用于第二计算设备，所述方法包括：

在包括n个计算单元的情况下，将样本数据划分为n个样本数据集合，每个样本数据集合包括至少一个样本数据，所述n为大于1的整数；

将所述n个样本数据集合分配给所述n个计算单元；

通过多个计算单元组中的每个计算单元，基于所述计算单元分配到的样本数据集合，并行训练联邦学习模型，每个计算单元组包括至少一个计算单元；

响应于目标计算单元组得到所述联邦学习模型的本地更新信息，向第一计算设备发送

所述目标计算单元组的本地更新信息，所述本地更新信息用于更新所述联邦学习模型，所述第一计算设备用于接收至少一个第二计算设备发送的本地更新信息，根据接收到的本地更新信息，确定全局更新信息，向至少一个第二计算设备发送所述全局更新信息；

接收所述全局更新信息，根据所述全局更新信息，更新所述联邦学习模型；

其中，所述通过多个计算单元组中的每个计算单元，基于所述计算单元分配到的样本数据集合，并行训练联邦学习模型，包括：

在所述n个计算单元中，确定至少一个目标计算单元；

将所述目标计算单元分配到的样本数据集合进行拆分，得到多个样本数据组，每个样本数据组包括至少一个样本数据；

通过所述目标计算单元，基于所述多个样本数据组中的每个样本数据组，分别对所述联邦学习模型进行迭代训练。

10.一种联邦学习装置，其特征在于，应用于模型训练系统，所述模型训练系统包括第一计算设备和多个第二计算设备，所述装置包括：

模型训练模块，用于在包括n个计算单元的情况下，将样本数据划分为n个样本数据集合，每个样本数据集合包括至少一个样本数据，所述n为大于1的整数；

所述模型训练模块，还用于将所述n个样本数据集合分配给所述n个计算单元；

所述模型训练模块，还用于通过多个计算单元组中的每个计算单元，基于所述计算单元分配到的样本数据集合，并行训练联邦学习模型，每个计算单元组包括至少一个计算单元；

本地信息发送模块，用于响应于本端的目标计算单元组得到所述联邦学习模型的本地更新信息，向所述第一计算设备发送所述目标计算单元组的本地更新信息，所述本地更新信息用于更新所述联邦学习模型，所述目标计算单元组为所述多个计算单元组中的任一个计算单元组；

全局信息发送模块，用于接收至少一个第二计算设备发送的本地更新信息，根据接收到的本地更新信息，确定全局更新信息，向至少一个第二计算设备发送所述全局更新信息；

所述模型训练模块，还用于接收所述全局更新信息，根据所述全局更新信息，更新本端的联邦学习模型；

其中，所述模型训练模块，还用于：

在所述n个计算单元中，确定至少一个目标计算单元；

将所述目标计算单元分配到的样本数据集合进行拆分，得到多个样本数据组，每个样本数据组包括至少一个样本数据；

通过所述目标计算单元，基于所述多个样本数据组中的每个样本数据组，分别对所述联邦学习模型进行迭代训练。

11.一种联邦学习装置，其特征在于，应用于第二计算设备，所述装置包括：

模型训练模块，用于在包括n个计算单元的情况下，将样本数据划分为n个样本数据集合，每个样本数据集合包括至少一个样本数据，所述n为大于1的整数；

所述模型训练模块，还用于将所述n个样本数据集合分配给所述n个计算单元；

所述模型训练模块，还用于通过多个计算单元组中的每个计算单元，基于所述计算单元分配到的样本数据集合，并行训练联邦学习模型，每个计算单元组包括至少一个计算单

元；

本地信息发送模块，用于响应于目标计算单元组得到所述联邦学习模型的本地更新信息，向第一计算设备发送所述目标计算单元组的本地更新信息，所述本地更新信息用于更新所述联邦学习模型，所述第一计算设备用于接收至少一个第二计算设备发送的本地更新信息，根据接收到的本地更新信息，确定全局更新信息，向至少一个第二计算设备发送所述全局更新信息；

所述模型训练模块，还用于接收所述全局更新信息，根据所述全局更新信息，更新所述联邦学习模型；

其中，所述模型训练模块，还用于：

在所述n个计算单元中，确定至少一个目标计算单元；

将所述目标计算单元分配到的样本数据集合进行拆分，得到多个样本数据组，每个样本数据组包括至少一个样本数据；

通过所述目标计算单元，基于所述多个样本数据组中的每个样本数据组，分别对所述联邦学习模型进行迭代训练。

12.一种计算设备，其特征在于，所述计算设备包括处理器和存储器，所述存储器中存储有至少一条计算机程序，所述至少一条计算机程序由所述处理器加载并执行，以实现如权利要求1至8任一项所述的联邦学习方法中所执行的操作，或者实现如权利要求9所述的联邦学习方法中所执行的操作。

13.一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中存储有至少一条计算机程序，所述至少一条计算机程序由处理器加载并执行，以实现如权利要求1至8任一项所述的联邦学习方法中所执行的操作，或者实现如权利要求9所述的联邦学习方法中所执行的操作。

联邦学习方法、装置、计算设备及存储介质

技术领域

[0001] 本申请实施例涉及计算机技术领域，特别涉及一种联邦学习方法、装置、计算设备及存储介质。

背景技术

[0002] 随着计算机技术的发展和人工智能技术的进步，联邦学习逐渐成为一个热门课题，联邦学习通过多方协作完成机器学习和深度学习模型的训练，在保护用户隐私和数据安全的同时，解决了数据孤岛的问题。

[0003] 联邦学习包括横向联邦学习，在横向联邦学习中，多个计算设备分别使用各自的样本数据共同训练同一个模型，但是由于各个计算设备的训练速度不同，训练速度较慢的计算设备会拉低整体的训练效率，导致难以支持高效的横向联邦学习。

发明内容

[0004] 本申请实施例提供了一种联邦学习方法、装置、计算设备及存储介质，能够提高联邦学习的效率。所述技术方案如下。

[0005] 一方面，提供了一种联邦学习方法，应用于模型训练系统，所述模型训练系统包括第一计算设备和多个第二计算设备，所述方法包括：

[0006] 所述第二计算设备通过本端的多个计算单元组，并行训练联邦学习模型，每个计算单元组包括至少一个计算单元；

[0007] 所述第二计算设备响应于本端的目标计算单元组得到所述联邦学习模型的本地更新信息，向所述第一计算设备发送所述目标计算单元组的本地更新信息，所述本地更新信息用于更新所述联邦学习模型，所述目标计算单元组为所述多个计算单元组中的任一个计算单元组；

[0008] 所述第一计算设备接收至少一个第二计算设备发送的本地更新信息，根据接收到的本地更新信息，确定全局更新信息，向至少一个第二计算设备发送所述全局更新信息；

[0009] 所述第二计算设备接收所述全局更新信息，根据所述全局更新信息，更新本端的联邦学习模型。

[0010] 可选地，所述第一计算设备接收至少一个第二计算设备发送的本地更新信息，根据接收到的本地更新信息，确定全局更新信息，向至少一个第二计算设备发送所述全局更新信息，包括：

[0011] 所述第一计算设备接收至少一个第二计算设备发送的本地更新信息，根据接收到的本地更新信息，确定全局更新信息，向每个第二计算设备发送所述全局更新信息；或者，

[0012] 所述第一计算设备接收多个第二计算设备发送的本地更新信息，根据接收到的本地更新信息，确定全局更新信息，向所述多个第二计算设备发送所述全局更新信息。

[0013] 另一方面，提供了一种联邦学习方法，应用于第二计算设备，所述方法包括：

[0014] 通过多个计算单元组，并行训练联邦学习模型，每个计算单元组包括至少一个计

算单元；

[0015] 响应于目标计算单元组得到所述联邦学习模型的本地更新信息，向第一计算设备发送所述目标计算单元组的本地更新信息，所述本地更新信息用于更新所述联邦学习模型，所述第一计算设备用于接收至少一个第二计算设备发送的本地更新信息，根据接收到的本地更新信息，确定全局更新信息，向至少一个第二计算设备发送所述全局更新信息；

[0016] 接收所述全局更新信息，根据所述全局更新信息，更新所述联邦学习模型。

[0017] 另一方面，提供了一种联邦学习装置，应用于模型训练系统，所述模型训练系统包括第一计算设备和多个第二计算设备，所述装置包括：

[0018] 模型训练模块，用于通过本端的多个计算单元组，并行训练联邦学习模型，每个计算单元组包括至少一个计算单元；

[0019] 本地信息发送模块，用于响应于本端的目标计算单元组得到所述联邦学习模型的本地更新信息，向所述第一计算设备发送所述目标计算单元组的本地更新信息，所述本地更新信息用于更新所述联邦学习模型，所述目标计算单元组为所述多个计算单元组中的任一个计算单元组；

[0020] 全局信息发送模块，用于接收至少一个第二计算设备发送的本地更新信息，根据接收到的本地更新信息，确定全局更新信息，向至少一个第二计算设备发送所述全局更新信息；

[0021] 所述模型训练模块，还用于接收所述全局更新信息，根据所述全局更新信息，更新本端的联邦学习模型。

[0022] 可选地，所述本地信息发送模块，包括：

[0023] 第一信息发送单元，用于在所述目标计算单元组包括多个计算单元的情况下，响应于所述目标计算单元组中的每个计算单元得到所述联邦学习模型的本地更新信息，向所述第一计算设备发送所述目标计算单元组中的每个计算单元的本地更新信息。

[0024] 可选地，所述本地信息发送模块，包括：

[0025] 第一融合单元，用于在所述目标计算单元组包括多个计算单元的情况下，所述第二计算设备响应于所述目标计算单元组中的每个计算单元得到所述联邦学习模型的本地更新信息，对所述目标计算单元组中的每个计算单元的本地更新信息进行融合，得到融合更新信息；

[0026] 第二信息发送单元，用于向所述第一计算设备发送所述融合更新信息。

[0027] 可选地，所述全局信息发送模块，包括：

[0028] 全局信息确定单元，用于接收目标数量的第二计算设备发送的本地更新信息，根据接收到的本地更新信息，确定所述全局更新信息；

[0029] 第三信息发送单元，用于向每个第二计算设备发送所述全局更新信息。

[0030] 可选地，所述全局信息发送模块，包括：

[0031] 轮次确定单元，用于接收目标数量的第二计算设备发送的本地更新信息，确定迭代轮次之差，所述迭代轮次之差为各个第二计算设备中最大的已迭代轮次与最小的已迭代轮次之差；

[0032] 全局信息确定单元，用于在所述迭代轮次之差不大于目标阈值的情况下，根据接收到的本地更新信息，确定所述全局更新信息；

[0033] 第三信息发送单元，用于向至少一个第二计算设备发送所述全局更新信息。

[0034] 可选地，所述全局信息确定单元，还用于在所述迭代轮次之差大于所述目标阈值的情况下，接收每个第二计算设备发送的每个计算单元的本地更新信息，根据接收到的本地更新信息，确定所述全局更新信息；

[0035] 所述第三信息发送单元，还用于向所述每个第二计算设备发送所述全局更新信息。

[0036] 可选地，所述模型训练模块，包括：

[0037] 样本数据划分单元，用于在所述第二计算设备包括n个计算单元的情况下，将样本数据划分为n个样本数据集合，每个样本数据集合包括至少一个样本数据，所述n为大于1的整数；

[0038] 样本数据分配单元，用于将所述n个样本数据集合分配给所述n个计算单元；

[0039] 模型训练单元，用于通过所述多个计算单元组中的每个计算单元，基于所述计算单元分配到的样本数据集合，并行训练所述联邦学习模型。

[0040] 可选地，所述模型训练单元，用于：

[0041] 在所述n个计算单元中，确定至少一个目标计算单元；

[0042] 将所述目标计算单元分配到的样本数据集合进行拆分，得到多个样本数据组，每个样本数据组包括至少一个样本数据；

[0043] 通过所述目标计算单元，基于所述多个样本数据组中的每个样本数据组，分别对所述联邦学习模型进行迭代训练。

[0044] 可选地，所述本地信息发送模块，包括：

[0045] 第一链路发送单元，用于响应于本端的目标计算单元组中的每个计算单元得到所述联邦学习模型的本地更新信息，通过所述第二计算设备与所述第一计算设备之间的网络链路，向所述第一计算设备发送所述目标计算单元组的本地更新信息；或者，

[0046] 第二链路发送单元，用于响应于本端的目标计算单元组中的每个计算单元得到所述联邦学习模型的本地更新信息，通过每个计算单元与所述第一计算设备之间的网络链路，分别向所述第一计算设备发送所述每个计算单元的本地更新信息；或者，

[0047] 第三链路发送单元，用于响应于本端的目标计算单元组中的每个计算单元得到所述联邦学习模型的本地更新信息，通过所述目标计算单元组与所述第一计算设备之间的网络链路，向所述第一计算设备发送所述目标计算单元组的本地更新信息。

[0048] 可选地，所述全局信息发送模块，用于：

[0049] 接收至少一个第二计算设备发送的本地更新信息，根据接收到的本地更新信息，确定全局更新信息，向每个第二计算设备发送所述全局更新信息；或者，

[0050] 接收多个第二计算设备发送的本地更新信息，根据接收到的本地更新信息，确定全局更新信息，向所述多个第二计算设备发送所述全局更新信息。

[0051] 可选地，所述全局信息发送模块，包括：

[0052] 第二融合单元，用于接收多个第二计算设备发送的本地更新信息，对接收到的多个本地更新信息进行融合，得到所述全局更新信息。

[0053] 另一方面，提供了一种联邦学习装置，应用于第二计算设备，所述装置包括：

[0054] 模型训练模块，用于通过多个计算单元组，并行训练联邦学习模型，每个计算单元

组包括至少一个计算单元；

[0055] 本地信息发送模块，用于响应于目标计算单元组得到所述联邦学习模型的本地更新信息，向第一计算设备发送所述目标计算单元组的本地更新信息，所述本地更新信息用于更新所述联邦学习模型，所述第一计算设备用于接收至少一个第二计算设备发送的本地更新信息，根据接收到的本地更新信息，确定全局更新信息，向至少一个第二计算设备发送所述全局更新信息；

[0056] 所述模型训练模块，还用于接收所述全局更新信息，根据所述全局更新信息，更新所述联邦学习模型。

[0057] 另一方面，提供了一种计算设备，所述计算设备包括处理器和存储器，所述存储器中存储有至少一条计算机程序，所述至少一条计算机程序由所述处理器加载并执行以实现如上述方面所述的联邦学习方法中所执行的操作。

[0058] 另一方面，提供了一种计算机可读存储介质，所述计算机可读存储介质中存储有至少一条计算机程序，所述至少一条计算机程序由处理器加载并执行以实现如上述方面所述的联邦学习方法中所执行的操作。

[0059] 另一方面，提供了一种计算机程序产品或计算机程序，所述计算机程序产品或计算机程序包括计算机程序代码，所述计算机程序代码存储在计算机可读存储介质中，计算设备的处理器从计算机可读存储介质读取所述计算机程序代码，处理器执行所述计算机程序代码，使得所述计算设备实现如上述方面所述的联邦学习方法中所执行的操作。

[0060] 本申请实施例提供的方法、装置、计算设备及存储介质，第二计算设备包括多个计算单元组，第二计算设备中的任意一个计算单元组通过训练联邦学习模型，得到本地更新信息，均可以向第一计算设备发送本地更新信息，第一计算设备根据本地更新信息确定全局更新信息。也即是第二计算设备采用基于计算单元组的方式，来向第一计算设备发送本地更新信息，无需等待所有计算单元组均得到本地更新信息，才能向第一计算设备发送本地更新信息，因此第二计算设备能够及时发送本地更新信息，从而及时参与到联邦学习模型的全局训练过程中，进而第一计算设备也能够及时确定全局更新信息，有利于提高整个联邦学习的效率。

附图说明

[0061] 为了更清楚地说明本申请实施例中的技术方案，下面将对实施例描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本申请实施例的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

[0062] 图1是本申请实施例提供的一种样本数据的示意图；

[0063] 图2是本申请实施例提供的一种模型训练系统的架构图；

[0064] 图3是本申请实施例提供的一种联邦学习方法的流程图；

[0065] 图4是本申请实施例提供的一种联邦学习方法的流程图；

[0066] 图5是本申请实施例提供的一种参数信息传输方法的示意图；

[0067] 图6是本申请实施例提供的一种参数信息传输方法的示意图；

[0068] 图7是本申请实施例提供的一种联邦学习方法的流程图；

[0069] 图8是本申请实施例提供的一种联邦学习装置的结构示意图；

[0070] 图9是本申请实施例提供的另一种联邦学习装置的结构示意图；

[0071] 图10是本申请实施例提供的另一种联邦学习装置的结构示意图；

[0072] 图11是本申请实施例提供的一种终端的结构示意图；

[0073] 图12是本申请实施例提供的一种服务器的结构示意图。

具体实施方式

[0074] 为使本申请实施例的目的、技术方案和优点更加清楚，下面将结合附图对本申请实施方式作进一步地详细描述。

[0075] 可以理解，本申请所使用的术语“第一”、“第二”等可在本文中用于描述各种概念，但除非特别说明，这些概念不受这些术语限制。这些术语仅用于将一个概念与另一个概念区分。举例来说，在不脱离本申请的范围的情况下，可以将第一计算设备称为第二计算设备，且类似地，可将第二计算设备称为第一计算设备。

[0076] 其中，至少一个是指一个或者一个以上，例如，至少一个计算单元可以是一个计算单元、两个计算单元、三个计算单元等任一大于等于一的整数个计算单元。多个是指两个或者两个以上，例如，多个计算单元可以是两个计算单元、三个计算单元等任一大于等于二的整数个计算单元。每个是指至少一个中的每一个，例如，每个计算单元是指多个计算单元中的每一个计算单元，若多个计算单元为3个计算单元，则每个计算单元是指3个计算单元中的每一个计算单元。

[0077] 人工智能(Artificial Intelligence,AI)是利用数字计算机或者数字计算机控制的机器模拟、延伸和扩展人的智能，感知环境、获取知识并使用知识获得最佳结果的理论、方法、技术及应用系统。换句话说，人工智能是计算机科学的一个综合技术，它企图了解智能的实质，并生产出一种新的能以人类智能相似的方式做出反应的智能机器。人工智能也就是研究各种智能机器的设计原理与实现方法，使机器具有感知、推理与决策的功能。

[0078] 人工智能技术是一门综合学科，涉及领域广泛，既有硬件层面的技术也有软件层面的技术。人工智能基础技术一般包括如传感器、专用人工智能芯片、云计算、分布式存储、大数据处理技术、操作/交互系统、机电一体化等技术。人工智能软件技术主要包括计算机视觉技术、语音处理技术、自然语言处理技术以及机器学习/深度学习、自动驾驶、智慧交通等几大方向。

[0079] 机器学习(Machine Learning,ML)是一门多领域交叉学科，涉及概率论、统计学、逼近论、凸分析、算法复杂度理论等多门学科。专门研究计算机怎样模拟或实现人类的学习行为，以获取新的知识或技能，重新组织已有的知识结构使之不断改善自身的性能。机器学习是人工智能的核心，是使计算机具有智能的根本途径，其应用遍及人工智能的各个领域。机器学习和深度学习通常包括人工神经网络、置信网络、强化学习、迁移学习、归纳学习、示教学习等技术。

[0080] 随着人工智能技术研究和进步，人工智能技术在多个领域展开研究和应用，例如常见的智能家居、智能穿戴设备、虚拟助理、智能音箱、智能营销、无人驾驶、自动驾驶、无人机、机器人、智能医疗、智能客服、车联网、自动驾驶、智慧交通等，相信随着技术的发展，人工智能技术将在更多的领域得到应用，并发挥越来越重要的价值。

[0081] 云技术(Cloud Technology)是指在广域网或局域网内将硬件、软件、网络等系列资源统一起来,实现数据的计算、储存、处理和共享的一种托管技术。云计算是指IT(Internet Technology,互联网技术)基础设施的交付和使用模式,指通过网络以按需、易扩展的方式获得所需资源;广义云计算指服务的交付和使用模式,指通过网络以按需、易扩展的方式获得所需服务。这种服务可以是IT和软件、互联网相关,也可是其他服务。云计算是网格计算(Grid Computing)、分布式计算(Distributed Computing)、并行计算(Parallel Computing)、效用计算(Utility Computing)、网络存储(Network Storage Technologies)、虚拟化(Virtualization)、负载均衡(Load Balance)等传统计算机和网络技术发展融合的产物。随着互联网、实时数据流、连接设备多样化的发展,以及搜索服务、社会网络、移动商务和开放协作等需求的推动,云计算迅速发展起来。不同于以往的并行分布式计算,云计算的产生从理念上将推动整个互联网模式、企业管理模式发生革命性的变革。

[0082] 以下将基于人工智能技术和云技术,对本申请实施例提供的联邦学习方法进行说明。

[0083] 为了便于理解本申请实施例提供的方法,对本申请涉及到的术语进行如下解释。

[0084] 联邦学习(Federated Learning):联邦学习又称为联合学习,能够在保护用户隐私和数据安全的前提下实现数据的“可用而不可见”,也即通过多方协作完成机器学习模型的训练任务,此外,还能够提供机器学习模型的推理服务。

[0085] 在人工智能时代,机器学习尤其深度学习模型的获得需要大量的训练数据作为前提。但是在很多业务场景中,模型的训练数据往往分散在各个不同的业务团队、部门、甚至是不同的公司内。为了确保用户隐私和数据安全,不同数据源之间不能够直接交换数据,形成了所谓的“数据孤岛”,阻碍了数据合作和获取模型所需要的大数据。近几年,联邦学习技术迅速发展,为跨部门、跨机构、跨行业数据合作提供了新的解决思路。联邦学习在保护用户隐私和数据安全的同时,充分利用多方数据源的数据来训练机器学习模型,通过使用多方、互补的数据源来提升机器学习模型的性能,例如,提升广告推荐模型的准确率。

[0086] 与传统的集中式机器学习不同,联邦学习过程中,由两个或两个以上的参与方一起协作训练一个或多个机器学习模型。从分类上来说,基于数据的分布特征,联邦学习可以划分为横向联邦学习(Horizontal Federated Learning)、纵向联邦学习(Vertical Federated Learning)和联邦迁移学习(Federated Transfer Learning)。其中,横向联邦学习又称为基于样本的联邦学习,适用于样本集共享相同特征空间但样本空间不同的情况;纵向联邦学习又称为基于特征的联邦学习,适用于样本集共享相同样本空间但特征空间不同的情况;联邦迁移学习则适用于样本集不仅在样本空间上不同而且在特征空间上也不同的情况。

[0087] 本申请实施例提供的联邦学习方法属于横向联邦学习方法,横向联邦学习的应用场景是联邦学习的各个计算设备中,各自的样本数据具有相同的特征空间和不同的样本空间,例如如图1所示,第二计算设备1、第二计算设备2和第二计算设备3中样本数据的特征空间均为特征1-特征L,但第二计算设备1中的样本空间为U1-U4,第二计算设备2中的样本空间为U5-U10,第二计算设备3中的样本空间为U11-U15。横向联邦学习的好处是能够增加整体的样本数据量。横向联邦学习的核心思想是让每个第二计算设备在本端使用各自拥有的样本数据训练一个模型,然后将多个第二计算设备所训练的模型进行融合,例如基于密码

学或者秘密分享技术进行安全模型融合(即安全聚合),从而得到一个联合多个第二计算设备的样本数据所训练的全局模型。

[0088] 本申请实施例提供的联邦学习方法,应用于模型训练系统,参见图2,该模型训练系统包括第一计算设备201和多个第二计算设备202,该第一计算设备201为服务器或者终端,该第二计算设备202为服务器、终端或者终端中运行的客户端等。其中,服务器是独立的物理服务器,或者是多个物理服务器构成的服务器集群或者分布式系统,或者是提供云服务、云数据库、云计算、云函数、云存储、网络服务、云通信、中间件服务、域名服务、安全服务、CDN(Content Delivery Network,内容分发网络)以及大数据和人工智能平台等基础云计算服务的云服务器。终端是智能手机、平板电脑、笔记本电脑、台式计算机、智能音箱、智能手表等,但并不局限于此。第一计算设备201以及第二计算设备202能够通过有线或无线通信方式进行直接或间接地连接,本申请在此不做限制。

[0089] 第一计算设备201和每个第二计算设备202中存储有联邦学习模型,且每个计算设备中存储的联邦学习模型的模型结构是相同的。每个第二计算设备202中还存储有各自的样本数据,不同的第二计算设备202中的样本数据具有相同的特征空间和不同的样本空间。

[0090] 每个第二计算设备202中运行有多个计算单元,其中,计算单元对应第二计算设备202中的一个或多个CPU(Central Processing Unit,中央处理器)核,或者计算单元对应第二计算设备202中的一个或多个GPU(Graphics Processing Unit,图形处理器)核。该多个计算单元是用于执行模型训练任务的计算单元,例如第一个第二计算设备202中运行计算单元1和计算单元2,第二个计算设备202中运行计算单元3和计算单元4,最后一个计算设备202中运行计算单元5、计算单元6和计算单元7等。每个第二计算设备202分别通过本端的各个计算单元,基于本端的样本数据并行训练联邦学习模型,并将某个计算单元的训练结果发送给第一计算设备201,由第一计算设备201将多个第二计算设备202的训练结果进行融合,根据融合结果更新每个第二计算设备202上的联邦学习模型。

[0091] 例如,每个第二计算设备202将本端的某个计算单元的训练联邦学习模型所得到的本地更新信息,发送给第一计算设备201。如图2所示,第一个计算设备202将计算单元1的本地更新信息$W_{1,1}$和计算单元2的本地更新信息$W_{1,2}$发送给第一计算设备201,第二个计算设备202将计算单元3的本地更新信息$W_{2,1}$和计算单元4的本地更新信息$W_{2,2}$发送给第一计算设备201,最后一个计算设备202将计算单元5的本地更新信息$W_{k,1}$、计算单元6的本地更新信息$W_{k,2}$和计算单元7的本地更新信息$W_{k,3}$发送给第一计算设备201。

[0092] 在一种可能实现方式中,将联邦学习系统应用于区块链,第一计算设备201和第二计算设备202分别为区块链中的不同节点,每个节点中存储有对应的样本数据。每个节点能够将训练的联邦学习模型存储在区块链中,之后该节点或者该区块链中的其他设备对应的节点可使用该联邦学习模型。

[0093] 其中,区块链是分布式数据存储、点对点传输、共识机制、加密算法等计算机技术的新型应用模式。区块链本质上是一个去中心化的数据库,是一串使用密码学方法相关联产生的数据块,每一个数据块中包含了一批次网络交易的信息,用于验证其信息的有效性(防伪)和生成下一个区块。区块链可以包括区块链底层平台、平台产品服务层以及应用服务层。其中,每个区块中包括本区块存储交易记录的哈希值(本区块的哈希值)、以及前一区

块的哈希值，各区块通过哈希值连接形成区块链。另外，区块中还可以包括有区块生成时的时间戳等信息。

[0094] 以分布式系统为区块链系统为例，由多个节点(接入网络中的任意形式的计算设备，如服务器、用户终端)和客户端形成，节点之间形成组成的点对点(P2P，Peer To Peer)网络，P2P协议是一个运行在传输控制协议(TCP，Transmission Control Protocol)协议之上的应用层协议。在分布式系统中，任何机器如服务器、终端都可以加入而成为节点，节点包括硬件层、中间层、操作系统层和应用层。

[0095] 本申请实施例提供的方法，可用于任一进行横向联邦学习的场景下，可以支持训练任意类型的机器学习模型或者深度学习模型，且每个计算设备在本端可以采用任意分布式的模型训练方法以及任意类型的模型训练框架。

[0096] 例如，在医疗领域中进行辅助问诊的场景下：第一计算设备为用于进行联邦学习的联邦服务器，多个第二计算设备分别为隶属于不同医院的应用服务器，每个应用服务器中存储有不同的患者对应的样本数据，例如样本数据为患者的病史信息或者主诉信息等。每个应用服务器采用本申请实施例提供的方法，分别通过本端的各个计算单元，基于本端的样本数据并行训练疾病预测模型，并将某个计算单元的训练结果发送给联邦服务器，由联邦服务器将多个应用服务器的训练结果进行融合，根据融合结果更新每个应用服务器上的疾病预测模型。之后基于训练的疾病预测模型对用户进行疾病预测，以便后续医生根据疾病预测结果结合用户的其他信息，来确定用户可能患有的疾病，从而在医生进行临床诊断过程中提供辅助性的决策。

[0097] 例如，物品推荐场景下：第一计算设备为用于进行联邦学习的联邦服务器，多个第二计算设备分别为不同的购物应用对应的应用服务器，每个应用服务器中存储有不同的用户标识对应的样本数据，例如样本数据包括用户标识对应的历史购物信息、历史浏览信息或者历史点击信息等。每个应用服务器采用本申请实施例提供的方法，分别通过本端的各个计算单元，基于本端的样本数据并行训练分类模型，并将某个计算单元的训练结果发送给联邦服务器，由联邦服务器将多个应用服务器的训练结果进行融合，根据融合结果更新每个应用服务器上的分类模型。之后基于训练的分类模型对用户进行分类，以便后续基于用户所属的类别来推荐符合其喜好的物品。

[0098] 在采用联邦学习方法训练模型的过程中，需要经过多次迭代过程，本申请实施例以任一次迭代过程为例，对模型的训练过程进行说明。

[0099] 图3是本申请实施例提供的一种联邦学习方法的流程图。本申请实施例应用于图2所示的模型训练系统中，该模型训练系统包括第一计算设备和多个第二计算设备，本申请实施例仅以任一第二计算设备和第一计算设备的一次交互过程为例，对模型的训练过程进行说明，参见图3，该方法包括以下步骤。

[0100] 301、第二计算设备通过本端的多个计算单元组，并行训练联邦学习模型。

[0101] 每个第二计算设备中运行有多个计算单元组，每个计算单元组包括至少一个计算单元，该多个计算单元用于执行模型训练的任务。其中，计算单元对应第二计算设备中的一个或多个CPU核，或者计算单元对应第二计算设备中的一个或多个GPU核。每个第二计算设备中存储有联邦学习模型，且每个联邦学习模型的模型结构相同，该联邦学习模型可以为任意类型的、执行任意任务的联邦学习模型。

[0102] 对于任一第二计算设备，该第二计算设备通过本端的多个计算单元组，并行训练本端的联邦学习模型。其中，由于每个计算单元组包括至少一个计算单元，因此第二计算设备是通过本端的每个计算单元组中的每个计算单元，并行训练本端的联邦学习模型。

[0103] 302、第二计算设备响应于本端的目标计算单元组得到联邦学习模型的本地更新信息，向第一计算设备发送目标计算单元组的本地更新信息。

[0104] 本地更新信息用于更新联邦学习模型，该本地更新信息是第二计算设备中的计算单元通过训练联邦学习模型所得到的，例如该本地更新信息为训练联邦学习模型所得到的模型参数，或者该本地更新信息为训练联邦学习模型所得到的梯度算子等，本申请实施例对此不做限定。

[0105] 其中，目标计算单元组为多个计算单元组中的任一个计算单元组，也即是第二计算设备中的任意一个计算单元组得到联邦学习模型的本地更新参数，第二计算设备均会向第一计算设备发送该计算单元组的本地更新信息。本申请实施例中，计算单元组包括至少一个计算单元，任意一个计算单元组得到本地更新信息，就可以向第一计算设备发送本地更新信息，也即是采用基于计算单元组的方式来向第一计算设备发送本地更新信息，无需第二计算设备中的所有计算单元组均得到本地更新信息，才能向第一计算设备发送本地更新信息，因此第二计算设备无需等待训练速度慢的计算单元组，能够及时发送本地更新信息，从而及时参与到联邦学习模型的全局训练过程中。

[0106] 303、第一计算设备接收至少一个第二计算设备发送的本地更新信息，根据接收到的本地更新信息，确定全局更新信息，向至少一个第二计算设备发送全局更新信息。

[0107] 模型训练系统包括多个第二计算设备，每个第二计算设备均会执行上述步骤301-302，从而向第一计算设备发送本端的计算单元组得到的本地更新信息，因此第一计算设备会不断接收到不同的第二计算设备发送的本地更新信息。第一计算设备接收至少一个第二计算设备发送的本地更新信息，则根据接收到的至少一个本地更新信息，确定全局更新信息，向至少一个第二计算设备发送该全局更新信息。

[0108] 其中，该全局更新信息也用于更新联邦学习模型。本地更新信息是第二计算设备中的计算单元组通过训练本端的联邦学习模型所得到的，训练本端的联邦学习模型所依据的数据是本端的样本数据，因此每个第二计算设备所得到的本地更新信息是基于本端的样本数据所得到的，如果第二计算设备仅根据本地更新信息，更新本端的联邦学习模型，则该联邦学习模型的训练过程仅参考了本端的样本数据，信息量较少，导致模型不够泛化。全局更新信息是第一计算设备根据至少一个第二计算设备发送的本地更新信息确定的，然后将该全局更新信息发送给至少一个第二计算设备，后续第二计算设备根据该全局更新信息，更新本端的联邦学习模型，则本端的联邦学习模型的整个训练过程相当于除了参考本端的样本数据，还能够参考其他第二计算设备中的样本数据，从而提高了样本数据的信息量，有利于提高模型的泛化性。

[0109] 304、第二计算设备接收全局更新信息，根据全局更新信息，更新本端的联邦学习模型。

[0110] 对于任一第二计算设备，该第二计算设备接收第一计算设备发送的全局更新信息，该全局更新信息参考了其他第二计算设备所得到的本地更新信息，相当于参考了其他第二计算设备中的样本数据，因此根据该全局更新信息，更新本端的联邦学习模型。因此在

模型训练系统中的每个第二计算设备，均能够参考其他第二计算设备中的样本数据，训练本端的联邦学习模型，最终每个第二计算设备中的联邦学习模型趋于收敛，每个第二计算设备训练得到相同的联邦学习模型，相当于利用多个第二计算设备中的样本数据，训练了一个全局的联邦学习模型。

[0111] 本申请实施例提供的方法，第二计算设备包括多个计算单元组，第二计算设备中的任意一个计算单元组通过训练联邦学习模型，得到本地更新信息，均可以向第一计算设备发送本地更新信息，第一计算设备根据本地更新信息确定全局更新信息。也即是第二计算设备采用基于计算单元组的方式，来向第一计算设备发送本地更新信息，无需等待所有计算单元组均得到本地更新信息，才能向第一计算设备发送本地更新信息，因此第二计算设备能够及时发送本地更新信息，从而及时参与到联邦学习模型的全局训练过程中，进而第一计算设备也能够及时确定全局更新信息，有利于提高整个联邦学习的效率。

[0112] 在采用联邦学习方法训练模型的过程中，需要经过多次迭代过程，本申请实施例以任一次迭代过程为例，对模型的训练过程进行说明。

[0113] 图4是本申请实施例提供的一种联邦学习方法的流程图。本申请实施例应用于图2所示的模型训练系统中，该模型训练系统包括第一计算设备和多个第二计算设备，本申请实施例仅以任一第二计算设备和第一计算设备的一次交互过程为例，对模型的训练过程进行说明，参见图4，该方法包括以下步骤。

[0114] 401、第二计算设备通过本端的多个计算单元组，并行训练联邦学习模型。

[0115] 每个第二计算设备中运行有多个计算单元组，每个计算单元组包括至少一个计算单元。每个第二计算设备中还存储有联邦学习模型和各自的样本数据，且每个第二计算设备中的联邦学习模型的模型结构相同，每个第二计算设备中的样本数据具有相同的特征空间和不同的样本空间。本申请实施例中，多个第二计算设备基于各自的样本数据，采用横向联邦学习的方式，共同训练联邦学习模型。其中，每个第二计算设备中存储的联邦学习模型可以称为“本地模型”，第一计算设备将多个第二计算设备训练的本地模型进行融合，所得到的联邦学习模型可以称为“全局模型”。每个本地模型具有相同的模型结构，在模型训练的各个阶段中，不同的本地模型的模型参数可能相同也可能不同，完成联合训练后，每个第二计算设备得到模型结构和模型参数均相同的全局模型。

[0116] 在一种可能实现方式中，在第二计算设备包括n个计算单元的情况下，第二计算设备将样本数据划分为n个样本数据集合，每个样本数据集合包括至少一个样本数据，n为大于1的整数。第二计算设备将n个样本数据集合分配给n个计算单元，通过多个计算单元组中的每个计算单元，基于计算单元分配到的样本数据集合，并行训练联邦学习模型。

[0117] 本申请实施例中，第二计算设备中的多个计算单元，采用并行模式进行分布式训练，每个计算单元均会得到一个样本数据集合，在一次迭代训练模型的过程中，每个计算单元基于分配到的样本数据集合，训练本端的联邦学习模型，各个计算单元间的训练过程互不影响。由于第二计算设备将样本数据划分为了n个样本数据集合，则每个计算单元分配到的样本数据集合各不相同，因此每个计算单元训练联邦学习模型所使用的样本数据集合均不相同，而多个计算单元之间是采用并行的方式训练联邦学习模型，也即是在同一时间分别使用不同样本数据集合训练联邦学习模型，能够提高在相同时间内训练模型所使用的数据量，有利于提高第二计算设备训练联邦学习模型的效率。

[0118] 可选地，第二计算设备在n个计算单元中，确定至少一个目标计算单元，将目标计算单元分配到的样本数据集合进行拆分，得到多个样本数据组，每个样本数据组包括至少一个样本数据。第二计算设备通过目标计算单元，基于多个样本数据组中的每个样本数据组，分别对联邦学习模型进行迭代训练。

[0119] 为了加快某些计算单元的训练速度，第二计算设备在n个计算单元中确定目标计算单元，将目标计算单元分配到的样本数据集合进行拆分，得到多个数据量更小的样本数据组。在通过目标计算单元进行一次迭代训练的过程中，基于多个样本数据组中的一个样本数据组，对联邦学习模型进行训练，在通过目标计算单元进行下一次迭代训练的过程中，则基于多个样本数据组中的下一个样本数据组，对联邦学习进行训练。也即是，对于目标计算单元来说，在一次迭代训练的过程中，仅使用一个样本数据组，而无需使用完整的样本数据集合，每次迭代训练时，依次轮换样本数据组，从而减少一次迭代训练过程中的数据量和运算量，加快了一次迭代训练的速度，有利于及时得到联邦学习模型的本地更新信息。

[0120] 对于除了目标计算单元之外的其他计算单元，则第二计算设备无需将样本数据集合进行拆分，在通过其他计算单元进行一次迭代训练的过程中，直接基于完整的样本数据集合，对联邦学习模型进行训练，在通过其他计算单元进行下一次迭代训练的过程中，继续基于完整的样本数据集合，对联邦学习模型进行训练。也即是，对于其他计算单元来说，在每次迭代训练的过程中，均使用完整的样本数据集合进行训练。

[0121] 可选地，在第二计算设备中仅包括一个计算单元的情况下，如果该第二计算设备的计算资源受限，导致处理速度较慢，则该第二计算设备也可以将样本数据拆分成多个数据量较小的样本数据组，在每次迭代训练过程中，仅使用一个样本数据组，并依次轮换多个样本数据组，以便计算资源受限的第二计算设备也能够及时向第一计算设备发送训练联邦学习模型所得到的本地更新信息。如果第二计算设备的计算资源丰富，处理速度较快，则第二计算设备在每次迭代训练过程中，均使用完整的样本数据，以便提高每次迭代训练过程中所使用的数据量。

[0122] 402、第二计算设备响应于本端的目标计算单元组得到联邦学习模型的本地更新信息，向第一计算设备发送目标计算单元组的本地更新信息。

[0123] 本地更新信息用于更新联邦学习模型，目标计算单元组为多个计算单元组中的任一个计算单元组。因此第二计算设备中的任意一个计算单元组得到联邦学习模型的本地更新参数，第二计算设备均会向第一计算设备发送该计算单元组的本地更新信息。由于第二计算设备无需等待所有计算单元组均得到本地更新信息，才能发送本地更新信息，因此能够保证可以及时向第一计算设备发送目标计算单元组中的计算单元所得到的本地更新信息，从而参与全局模型的训练，避免由于某些计算单元组的训练速度较慢，导致第二计算设备无法及时参与到全局模型的训练中。

[0124] 其中，本地更新信息是通过训练联邦学习模型得到的。在一种可能实现方式中，对于每个计算单元，在一次迭代训练过程中，使用多个样本数据进行训练，则计算单元在一次迭代训练过程中会得到每个样本数据对应的更新信息，将多个样本数据对应的更新信息进行加权平均，得到本次迭代训练过程中的本地更新信息。例如本地更新信息为模型参数或者梯度算子等。

[0125] 在一种可能实现方式中，每个计算单元组包括多个计算单元，则第二计算设备响

应于本端的任意一个计算单元得到联邦学习模型的本地更新信息，确定该计算单元所在的计算单元组中的其他计算单元是否得到本地更新信息，如果其他计算单元均得到本地更新信息，也即是该计算单元组中的每个计算单元均得到本地更新信息，则第二计算设备向第一计算设备发送该计算单元组的本地更新信息。如果其他计算单元中至少存在一个计算单元没有得到本地更新信息，则第二计算设备先不向第一计算设备发送本地更新信息，继续等待未得到本地更新信息的其他计算单元，直至该计算单元组中的每个计算单元均得到本地更新信息，则向第一计算设备发送该计算单元组的本地更新信息。

[0126] 在另一种可能实现方式中，每个计算单元组包括一个计算单元，则第二计算设备响应于本端的任意一个计算单元得到联邦学习模型的本地更新信息，向第一计算设备发送该计算单元的本地更新信息。在每个计算单元组包括一个计算单元的情况下，相当于以计算单元为单位，向第一设备发送本地更新信息，相比于每个计算单元组包括多个计算单元，此种情况下每个计算单元发送本地更新信息的过程也互不影响，能够进一步提高第二计算设备向第一计算设备发送本地更新信息的频率。例如，第二计算设备包括n个计算单元，n为大于1的整数，当第二计算设备的第j个计算单元得到联邦学习模型的本地更新信息，则通过该第j个计算单元向第一计算设备发送该本地更新信息，j为不大于n的正整数。

[0127] 本申请实施例中，第二计算设备包括多个计算单元，对多个计算单元进行划分得到多个计算单元组，由于每个计算单元组包括多少计算单元可以灵活设置，因此通过划分计算单元组，能够灵活控制每次向第一计算设备发送多少个计算单元的本地更新信息。由于每个计算单元组包括的计算单元越多，每次向第一计算设备发送的信息量也越多，但是向第一计算设备发送本地更新信息的频率会相对较低；每个计算单元组包括的计算单元越少，向第一计算设备发送本地更新信息的频率越高，但是每次向第一计算设备发送的信息量会相对较少，因此通过划分计算单元组，能够灵活控制向第一计算设备发送本地更新信息的频率以及信息量。

[0128] 在另一种可能实现方式中，在目标计算单元组包括多个计算单元的情况下，第二计算设备响应于目标计算单元组中的每个计算单元得到联邦学习模型的本地更新信息，向第一计算设备发送目标计算单元组中的每个计算单元的本地更新信息。

[0129] 如果目标计算单元组包括多个计算单元，则每个计算单元均会得到本地更新信息，因此目标计算单元组会包括多个本地更新信息，则每次向第一计算设备发送目标计算单元组的本地更新信息是指，向第一计算设备发送该多个本地更新信息。例如，第二计算设备将多个本地更新信息进行打包，将打包后的多个本地更新信息同时发送给第一计算设备。

[0130] 在另一种可能实现方式中，在目标计算单元组包括多个计算单元的情况下，第二计算设备响应于目标计算单元组中的每个计算单元得到联邦学习模型的本地更新信息，对目标计算单元组中的每个计算单元的本地更新信息进行融合，得到融合更新信息；向第一计算设备发送融合更新信息。

[0131] 如果目标计算单元组包括多个计算单元，则每个计算单元均会得到本地更新信息，因此目标计算单元组会包括多个本地更新信息，则每次向第一计算设备发送目标计算单元组的本地更新信息是指，向第一计算设备发送该多个本地更新信息融合后的融合更新信息。例如，第一计算设备采用加权平均的方式对多个本地更新信息进行融合，得到融合更

新信息。

[0132] 在另一种可能实现方式中，第二计算设备响应于本端的目标计算单元组中的每个计算单元得到联邦学习模型的本地更新信息，通过第二计算设备与第一计算设备之间的网络链路，向第一计算设备发送目标计算单元组的本地更新信息。

[0133] 第二计算设备与第一计算设备之间建立有网络链路，则目标计算单元组中的每个计算单元，均通过该网络链路，向第一计算设备发送本地更新信息。

[0134] 在另一种可能实现方式中，第二计算设备响应于本端的目标计算单元组中的每个计算单元得到联邦学习模型的本地更新信息，通过每个计算单元与第一计算设备之间的网络链路，分别向第一计算设备发送每个计算单元的本地更新信息；

[0135] 第二计算设备中的每个计算单元与第一计算设备之间均建立有网络链路，则目标计算单元组中的每个计算单元，通过各自的网络链路，分别向第一计算设备发送本地更新信息。

[0136] 在另一种可能实现方式中，第二计算设备响应于本端的目标计算单元组中的每个计算单元得到联邦学习模型的本地更新信息，通过目标计算单元组与第一计算设备之间的网络链路，向第一计算设备发送目标计算单元组的本地更新信息。

[0137] 第二计算设备中的每个计算单元组与第一计算设备之间建立有网络链路，则目标计算单元组中的每个计算单元，均通过该目标计算单元组的网络链路，向第一计算设备发送本地更新信息。

[0138] 在另一种可能实现方式中，第二计算设备响应于本端的目标计算单元组得到联邦学习模型的本地更新信息，将本地更新信息拆分成多个本地更新子信息，依次向第一计算设备发送每个本地更新子信息。

[0139] 如果第二计算设备的网络资源受限，导致第二计算设备的传输速度较慢，或者联邦学习模型的模型参数较多，则可以将本地更新信息拆分成多个本地更新子信息，每次只发送一个本地更新子信息，从而将本地更新信息分批次发送给第一计算设备，以便能够及时向第一计算设备发送部分本地更新信息，及时参与到全局模型的训练过程中。

[0140] 403、第一计算设备接收至少一个第二计算设备发送的本地更新信息，根据接收到的本地更新信息，确定全局更新信息，向至少一个第二计算设备发送全局更新信息。

[0141] 模型训练系统包括多个第二计算设备，每个第二计算设备均会执行上述步骤401-402，从而向第一计算设备发送本端的计算单元组得到的本地更新信息，因此第一计算设备会接收到不同的第二计算设备发送的本地更新信息。第一计算设备接收至少一个第二计算设备发送的本地更新信息，则根据接收到的至少一个本地更新信息，确定全局更新信息，向至少一个第二计算设备发送该全局更新信息，以便第二计算设备根据全局更新信息，更新联邦学习模型。

[0142] 在一种可能实现方式中，第一计算设备接收多个第二计算设备发送的本地更新信息，对接收到的多个本地更新信息进行融合，得到全局更新信息。可选地，第一计算设备采用联邦平均、安全聚合或者加权平均等方式，对多个本地更新信息进行融合，得到全局更新信息。

[0143] 在另一种可能实现方式中，在横向联邦学习中，第一计算设备可以采用同步并行(Bulk Synchronous Parallel，BSP)、异步并行(Asynchronous Parallel，ASP)或延迟异步

并行(Stalness Synchronous Parallel,SSP)等方式来协调多个第二计算设备的本地更新信息,来进行信息融合。

[0144] (1)同步并行模式:第一计算设备接收每个第二计算设备发送的每个计算单元的本地更新信息,根据接收到的本地更新信息,确定全局更新信息。

[0145] 在同步并行模式下,第一计算设备在接收到每个第二计算设备发送的每个计算单元的本地更新信息之后,才会更新全局更新信息,因此第一计算设备需要等待每个计算单元的本地更新信息。同步并行模式能够保证全局更新信息的收敛性,全局更新信息用于更新联邦学习模型,进而能够保证联邦学习模型的收敛性。

[0146] (2)异步并行模式:第一计算设备接收目标数量的第二计算设备发送的本地更新信息,根据接收到的本地更新信息,确定全局更新信息。

[0147] 在异步并行模式下,第一计算设备在接收到目标数量的第二计算设备的本地参数信息更新之后,更新全局参数信息,例如目标数量为1、5或者10等,因此第一计算设备不需要等待所有的第二计算设备发送本地更新信息。异步并行模式规避了等待训练速度较慢的第二计算设备的问题,能够加速全局参数信息的更新流程,从而减少联邦学习模型的训练时长。

[0148] (3)延迟同步并行模式:第一计算设备接收目标数量的第二计算设备发送的本地更新信息,确定迭代轮次之差,迭代轮次之差为各个第二计算设备中最大的已迭代轮次与最小的已迭代轮次之差;第一计算设备在迭代轮次之差不大于目标阈值的情况下,根据接收到的本地更新信息,确定全局更新信息,向至少一个第二计算设备发送全局更新信息。或者,第一计算设备在迭代轮次之差大于目标阈值的情况下,接收每个第二计算设备发送的每个计算单元的本地更新信息,根据接收到的本地更新信息,确定全局更新信息,向每个第二计算设备发送全局更新信息。

[0149] 延迟同步并行模式是一种同步并行模式和异步并行模式相结合的方式,在延迟同步并行模式下,根据迭代轮次之差来确定采用同步并行模式还是异步并行模式。其中,最大的已迭代轮次对应的第二计算设备是迭代速度最快的,最小的已迭代轮次对应的第二计算设备是迭代速度最慢的,如果最大的已迭代轮次与最小的已迭代轮次之差不大于目标阈值,则采用异步并行模式,根据接收到的目标数量的本地更新信息,确定全局更新信息,无需等待其他第二计算设备中的计算单元。如果最大的已迭代轮次与最小的已迭代轮次之差大于目标阈值,则采用同步并行模式,接收到目标数量的本地更新信息后,继续等待其他第二计算设备的计算单元,在接收到每个第二计算设备发送的每个计算单元的本地更新信息,则根据接收到的多个本地更新信息,确定全局更新信息。

[0150] 本申请实施例所说的已迭代轮次,是指从上一次采用同步并行模式开始到现在,各个第二计算设备的已迭代轮次。每当最大的已迭代轮次与最小的已迭代轮次之差大于目标阈值,则采用同步并行模式更新一次。也即是,在一段时间内,阶段性地采用异步并行模式和同步并行模式相交替的方式进行更新。可选地,每当最大的已迭代轮次与最小的已迭代轮次之差大于目标阈值,则采用同步并行模式更新目标次数,然后再采用异步并行模式,直至最大的已迭代轮次与最小的已迭代轮次之差大于目标阈值,继续更换为同步并行模式。由于异步并行模式能够加快模型的训练速度,同步并行模式能够提高模型的收敛性,因此采用延迟同步并行模式,能够平衡模型的训练速度以及模型的收敛性。

[0151] 在另一种可能实现方式中，第一计算设备接收至少一个第二计算设备发送的本地更新信息，根据接收到的本地更新信息，确定全局更新信息，向每个第二计算设备发送全局更新信息。

[0152] 第二计算设备的本地更新信息是基于本端的样本数据，训练联邦学习模型所得到的，每个第二计算设备中存储的样本数据不相同，因此得到的本地更新信息也不同。第一计算设备根据至少一个第二计算设备的本地更新信息，确定全局更新信息，则该全局更新信息参考了至少一个第二计算设备的本地更新信息，相当于参考了该至少一个第二计算设备的样本数据，则第一计算设备向每个第二计算设备发送该全局更新信息，以便根据该全局更新信息，更新本端的联邦学习模型，因此每个第二计算设备中联邦学习模型的更新过程，不仅能够参考本端的样本数据，还能够参考其他第二计算设备中的样本数据，相当于提高了联邦学习模型对应的样本数据的数据量，有利于提高联邦学习模型的泛化性。

[0153] 在另一种可能实现方式中，第一计算设备接收多个第二计算设备发送的本地更新信息，根据接收到的本地更新信息，确定全局更新信息，向该多个第二计算设备发送全局更新信息。其中，该多个第二计算设备的数量可以由模型训练系统来确定，或者由第一计算设备动态确定，或者根据预先设定的更新规则来确定，本申请实施例对此不做限定。

[0154] 第一计算设备根据多个第二计算设备的本地更新信息，确定全局更新信息，则该全局更新信息参考了多个第二计算设备的本地更新信息，相当于参考了该多个第二计算设备的样本数据，因此相对于单个的本地更新信息，该全局更新信息的泛化性更好，则第一计算设备向该多个第二计算设备发送该全局更新信息，以便根据该全局更新信息，更新本端的联邦学习模型，因此该多个第二计算设备中联邦学习模型的更新过程能够相互借鉴，不仅参考了本端的样本数据，还参考了其他第二计算设备中的样本数据，相当于提高了联邦学习模型对应的样本数据的数据量，有利于提高联邦学习模型的泛化性。

[0155] 404、第二计算设备接收全局更新信息，根据全局更新信息，更新本端的联邦学习模型。

[0156] 对于任一第二计算设备，该第二计算设备根据该全局更新信息，更新本端的联邦学习模型。因此在模型训练系统中的每个第二计算设备，均能够参考其他第二计算设备中的样本数据，训练本端的联邦学习模型，最终每个第二计算设备中的联邦学习模型趋于收敛，每个第二计算设备训练得到相同的联邦学习模型，相当于利用多个第二计算设备中的样本数据，训练了一个全局的联邦学习模型。

[0157] 在一种可能实现方式中，为了保证数据的安全性，采用加密算法来传输更新信息，如图5所示，则上述步骤402-404由以下步骤501-503代替。

[0158] 501、第二计算设备响应于本端的目标计算单元组得到联邦学习模型的本地更新信息，对目标计算单元组的本地更新信息进行加密，得到加密后的本地更新信息，向第一计算设备发送加密后的本地更新信息。

[0159] 502、第一计算设备接收至少一个第二计算设备发送的加密后的本地更新信息，根据接收到的加密后的本地更新信息，确定加密后的全局更新信息，向至少一个第二计算设备发送加密后的全局更新信息。

[0160] 503、第二计算设备接收加密后的全局更新信息，对加密后的全局更新信息进行解密，得到解密后的全局更新信息，根据解密后的全局更新信息，更新本端的联邦学习模型。

[0161] 如图6所示，为了保证本地更新信息的安全性和隐私性，第二计算设备602在获取到本地更新信息后，先采用加密算法将本地更新信息进行加密，向第一计算设备601发送加密后的本地更新信息。第一计算设备601接收到加密后的本地更新信息后，无需对加密后的本地更新信息进行解密，直接采用同态加密等安全聚合的方式，对接收到的加密后的本地更新信息进行融合，得到加密后的全局更新信息，并发送给第二计算设备602。第二计算设备602采用与加密算法对应的解密算法，对加密后的全局更新信息进行解密，得到解密后的全局更新信息。其中，加密算法和对应的解密算法仅存储于第二计算设备602中，第一计算设备601中未存储加密算法和对应的解密算法，第一计算设备601无需也无法对加密后的本地更新信息或者全局更新信息进行解密，因此能够保证本地更新信息和全局更新信息的安全性和隐私性。

[0162] 本申请实施例提出了一种基于计算单元组并行更新的横向联邦学习方法，以图2所示的模型训练系统包括一个第一计算设备和k个第二计算设备为例，k为大于1的整数。每个第二计算设备拥有多个计算单元，多个计算单元之间采用并行的方式对联邦学习模型进行分布式训练。以一个计算单元组包括一个计算单元为例，则每个第二计算设备以计算单元为最小单位，向第一计算设备发送计算单元得到的本地更新信息。对于不同的第二计算设备的不同计算单元，第一计算设备采用同步并行模式、异步并行模式或者延迟同步并行模式，来确定全局更新信息。在异步并行模式或者延迟同步并行模式下，基于计算单元并行更新的横向联邦学习方法，能够避免因为计算资源或者网络资源的限制，导致部分第二计算设备无法及时参与全局模型的训练的情况，有利于提高联邦学习模型的训练效率。

[0163] 需要说明的是，本申请实施例仅以一个第二计算设备向第一计算设备发送一次本地更新信息为例进行说明，在训练联邦学习模型的过程中，每个第二计算设备均会向第一计算设备发送本地更新信息，且每个第二计算设备会进行多次迭代，向第一计算设备发送多次本地更新信息，第一计算设备也会进行多次迭代，向第二计算设备发送多次全局更新信息。在一种可能实现方式中，响应于第一计算设备的迭代轮次达到第一阈值，停止对联邦学习模型进行训练；或者响应于每个第二计算设备在当前迭代轮次得到的损失值不大于第二阈值，停止对联邦学习模型进行训练。其中，第一阈值和第二阈值均为任意的数值，例如，第一阈值为100或150等，第二阈值为0.01或0.03等。

[0164] 本申请实施例提供的方法，第二计算设备包括多个计算单元组，第二计算设备中的任意一个计算单元组通过训练联邦学习模型，得到本地更新信息，均可以向第一计算设备发送本地更新信息，第一计算设备根据本地更新信息确定全局更新信息。也即是第二计算设备采用基于计算单元组的方式，来向第一计算设备发送本地更新信息，无需等待所有计算单元组均得到本地更新信息，才能向第一计算设备发送本地更新信息，因此第二计算设备能够及时发送本地更新信息，从而及时参与到联邦学习模型的全局训练过程中，进而第一计算设备也能够及时确定全局更新信息，有利于提高整个联邦学习的效率。

[0165] 并且，将样本数据划分为了n个样本数据集合，则每个计算单元分配到的样本数据集合各不相同，因此每个计算单元训练联邦学习模型所使用的样本数据集合均不相同，而多个计算单元之间是采用并行的方式训练联邦学习模型，也即是在同一时间分别使用不同样本数据集合训练联邦学习模型，能够提高在相同时间内训练模型所使用的数据量，有利于提高第二计算设备训练联邦学习模型的效率。

[0166] 并且，对于目标计算单元来说，在一次迭代训练的过程中，仅使用一个样本数据组，而无需使用完整的样本数据集合，每次迭代训练时，依次轮换样本数据组，从而减少一次迭代训练过程中的数据量和运算量，加快了一次迭代训练的速度，有利于及时得到联邦学习模型的本地更新信息。

[0167] 图7是本申请实施例提供的一种联邦学习方法的流程图。本申请实施例应用于图2所示的模型训练系统中的第二计算设备，参见图7，该方法包括以下步骤。

[0168] 701、第二计算设备通过多个计算单元组，并行训练联邦学习模型。

[0169] 702、第二计算设备响应于目标计算单元组得到联邦学习模型的本地更新信息，向第一计算设备发送目标计算单元组的本地更新信息。

[0170] 本地更新信息用于更新联邦学习模型，第一计算设备用于接收至少一个第二计算设备发送的本地更新信息，根据接收到的本地更新信息，确定全局更新信息，向至少一个第二计算设备发送全局更新信息。

[0171] 步骤701-702与上述步骤401-402同理，在此不再一一赘述。

[0172] 703、第二计算设备接收全局更新信息，根据全局更新信息，更新联邦学习模型。

[0173] 步骤703与上述步骤404同理，在此不再一一赘述。

[0174] 本申请实施例提供的方法，第二计算设备包括多个计算单元组，第二计算设备中的任意一个计算单元组通过训练联邦学习模型，得到本地更新信息，均可以向第一计算设备发送本地更新信息，由第一计算设备根据本地更新信息确定全局更新信息。也即是第二计算设备采用基于计算单元组的方式，来向第一计算设备发送本地更新信息，无需等待所有计算单元组均得到本地更新信息，才能向第一计算设备发送本地更新信息，因此第二计算设备能够及时发送本地更新信息，从而及时参与到联邦学习模型的全局训练过程中。

[0175] 图8是本申请实施例提供的一种联邦学习装置的结构示意图。参见图8，该装置应用于模型训练系统，模型训练系统包括第一计算设备和多个第二计算设备，该装置包括：

[0176] 模型训练模块801，用于通过本端的多个计算单元组，并行训练联邦学习模型，每个计算单元组包括至少一个计算单元；

[0177] 本地信息发送模块802，用于响应于本端的目标计算单元组得到联邦学习模型的本地更新信息，向第一计算设备发送目标计算单元组的本地更新信息，本地更新信息用于更新联邦学习模型，目标计算单元组为多个计算单元组中的任一个计算单元组；

[0178] 全局信息发送模块803，用于接收至少一个第二计算设备发送的本地更新信息，根据接收到的本地更新信息，确定全局更新信息，向至少一个第二计算设备发送全局更新信息；

[0179] 模型训练模块801，还用于接收全局更新信息，根据全局更新信息，更新本端的联邦学习模型。

[0180] 本申请实施例提供的联邦学习装置，任意一个计算单元组通过训练联邦学习模型，得到本地更新信息，均可以向第一计算设备发送本地更新信息，根据本地更新信息确定全局更新信息。也即是采用基于计算单元组的方式，来向第一计算设备发送本地更新信息，无需等待所有计算单元组均得到本地更新信息，才能向第一计算设备发送本地更新信息，因此能够及时发送本地更新信息，从而及时参与到联邦学习模型的全局训练过程中，进而也能够及时确定全局更新信息，有利于提高整个联邦学习的效率。

[0181] 可选地，参见图9，本地信息发送模块802，包括：

[0182] 第一信息发送单元812，用于在目标计算单元组包括多个计算单元的情况下，响应于目标计算单元组中的每个计算单元得到联邦学习模型的本地更新信息，向第一计算设备发送目标计算单元组中的每个计算单元的本地更新信息。

[0183] 可选地，参见图9，本地信息发送模块802，包括：

[0184] 第一融合单元822，用于在目标计算单元组包括多个计算单元的情况下，第二计算设备响应于目标计算单元组中的每个计算单元得到联邦学习模型的本地更新信息，对目标计算单元组中的每个计算单元的本地更新信息进行融合，得到融合更新信息；

[0185] 第二信息发送单元832，用于向第一计算设备发送融合更新信息。

[0186] 可选地，参见图9，全局信息发送模块803，包括：

[0187] 全局信息确定单元813，用于接收目标数量的第二计算设备发送的本地更新信息，根据接收到的本地更新信息，确定全局更新信息；

[0188] 第三信息发送单元823，用于向每个第二计算设备发送全局更新信息。

[0189] 可选地，参见图9，全局信息发送模块803，包括：

[0190] 轮次确定单元833，用于接收目标数量的第二计算设备发送的本地更新信息，确定迭代轮次之差，迭代轮次之差为各个第二计算设备中最大的已迭代轮次与最小的已迭代轮次之差；

[0191] 全局信息确定单元813，用于在迭代轮次之差不大于目标阈值的情况下，根据接收到的本地更新信息，确定全局更新信息；

[0192] 第三信息发送单元823，用于向至少一个第二计算设备发送全局更新信息。

[0193] 可选地，参见图9，全局信息确定单元813，还用于在迭代轮次之差大于目标阈值的情况下，接收每个第二计算设备发送的每个计算单元的本地更新信息，根据接收到的本地更新信息，确定全局更新信息；

[0194] 第三信息发送单元823，还用于向每个第二计算设备发送全局更新信息。

[0195] 可选地，参见图9，模型训练模块801，包括：

[0196] 样本数据划分单元811，用于在第二计算设备包括n个计算单元的情况下，将样本数据划分为n个样本数据集合，每个样本数据集合包括至少一个样本数据，n为大于1的整数；

[0197] 样本数据分配单元821，用于将n个样本数据集合分配给n个计算单元；

[0198] 模型训练单元831，用于通过多个计算单元组中的每个计算单元，基于计算单元分配到的样本数据集合，并行训练联邦学习模型。

[0199] 可选地，参见图9，模型训练单元831，用于：

[0200] 在n个计算单元中，确定至少一个目标计算单元；

[0201] 将目标计算单元分配到的样本数据集合进行拆分，得到多个样本数据组，每个样本数据组包括至少一个样本数据；

[0202] 通过目标计算单元，基于多个样本数据组中的每个样本数据组，分别对联邦学习模型进行迭代训练。

[0203] 可选地，参见图9，本地信息发送模块802，包括：

[0204] 第一链路发送单元842，用于响应于本端的目标计算单元组中的每个计算单元得

到联邦学习模型的本地更新信息，通过第二计算设备与第一计算设备之间的网络链路，向第一计算设备发送目标计算单元组的本地更新信息；或者，

[0205] 第二链路发送单元852，用于响应于本端的目标计算单元组中的每个计算单元得到联邦学习模型的本地更新信息，通过每个计算单元与第一计算设备之间的网络链路，分别向第一计算设备发送每个计算单元的本地更新信息；或者，

[0206] 第三链路发送单元862，用于响应于本端的目标计算单元组中的每个计算单元得到联邦学习模型的本地更新信息，通过目标计算单元组与第一计算设备之间的网络链路，向第一计算设备发送目标计算单元组的本地更新信息。

[0207] 可选地，参见图9，全局信息发送模块803，用于：

[0208] 接收至少一个第二计算设备发送的本地更新信息，根据接收到的本地更新信息，确定全局更新信息，向每个第二计算设备发送全局更新信息；或者，

[0209] 接收多个第二计算设备发送的本地更新信息，根据接收到的本地更新信息，确定全局更新信息，向该多个第二计算设备发送全局更新信息。

[0210] 可选地，参见图9，全局信息发送模块803，包括：

[0211] 第二融合单元843，用于接收多个第二计算设备发送的本地更新信息，对接收到的多个本地更新信息进行融合，得到全局更新信息。

[0212] 需要说明的是：上述实施例提供的联邦学习装置在进行联邦学习时，仅以上述各功能模块的划分进行举例说明，实际应用中，可以根据需要而将上述功能分配由不同的功能模块完成，即将计算设备的内部结构划分成不同的功能模块，以完成以上描述的全部或者部分功能。另外，上述实施例提供的联邦学习装置与联邦学习方法实施例属于同一构思，其具体实现过程详见方法实施例，这里不再赘述。

[0213] 图10是本申请实施例提供的一种联邦学习装置的结构示意图。参见图10，该装置应用于第二计算设备，该装置包括：

[0214] 模型训练模块1001，用于通过多个计算单元组，并行训练联邦学习模型，每个计算单元组包括至少一个计算单元；

[0215] 本地信息发送模块1002，用于响应于目标计算单元组得到联邦学习模型的本地更新信息，向第一计算设备发送目标计算单元组的本地更新信息，本地更新信息用于更新联邦学习模型，第一计算设备用于接收至少一个第二计算设备发送的本地更新信息，根据接收到的本地更新信息，确定全局更新信息，向至少一个第二计算设备发送全局更新信息；

[0216] 模型训练模块1001，还用于接收全局更新信息，根据全局更新信息，更新联邦学习模型。

[0217] 本申请实施例提供的联邦学习装置，任意一个计算单元组通过训练联邦学习模型，得到本地更新信息，均可以向第一计算设备发送本地更新信息，根据本地更新信息确定全局更新信息。也即是采用基于计算单元组的方式，来向第一计算设备发送本地更新信息，无需等待所有计算单元组均得到本地更新信息，才能向第一计算设备发送本地更新信息，因此能够及时发送本地更新信息，从而及时参与到联邦学习模型的全局训练过程中。

[0218] 需要说明的是：上述实施例提供的联邦学习装置在进行联邦学习时，仅以上述各功能模块的划分进行举例说明，实际应用中，可以根据需要而将上述功能分配由不同的功能模块完成，即将计算设备的内部结构划分成不同的功能模块，以完成以上描述的全部或

者部分功能。另外，上述实施例提供的联邦学习装置与联邦学习方法实施例属于同一构思，其具体实现过程详见方法实施例，这里不再赘述。

[0219] 本申请实施例还提供了一种计算设备，该计算设备包括处理器和存储器，存储器中存储有至少一条计算机程序，该至少一条计算机程序由处理器加载并执行，以实现上述实施例的联邦学习方法中所执行的操作。

[0220] 可选地，该计算设备提供为终端。图11示出了本申请一个示例性实施例提供的终端1100的结构示意图。

[0221] 终端1100包括有：处理器1101和存储器1102。

[0222] 处理器1101可以包括一个或多个处理核心，比如4核心处理器、8核心处理器等。处理器1101可以采用DSP(Digital Signal Processing，数字信号处理)、FPGA(Field Programmable Gate Array，现场可编程门阵列)、PLA(Programmable Logic Array，可编程逻辑阵列)中的至少一种硬件形式来实现。处理器1101也可以包括主处理器和协处理器，主处理器是用于对在唤醒状态下的数据进行处理的处理器，也称CPU(Central Processing Unit，中央处理器)；协处理器是用于对在待机状态下的数据进行处理的低功耗处理器。在一些实施例中，处理器1101可以集成有GPU(Graphics Processing Unit，图像处理的交互器)，GPU用于负责显示屏所需要显示的内容的渲染和绘制。一些实施例中，处理器1101还可以包括AI(Artificial Intelligence，人工智能)处理器，该AI处理器用于处理有关机器学习的计算操作。

[0223] 存储器1102可以包括一个或多个计算机可读存储介质，该计算机可读存储介质可以是非暂态的。存储器1102还可包括高速随机存取存储器，以及非易失性存储器，比如一个或多个磁盘存储设备、闪存存储设备。在一些实施例中，存储器1102中的非暂态的计算机可读存储介质用于存储至少一条计算机程序，该至少一条计算机程序用于被处理器1101所具有以实现本申请中方法实施例提供的联邦学习方法。

[0224] 在一些实施例中，终端1100还可选包括有：外围设备接口1103和至少一个外围设备。处理器1101、存储器1102和外围设备接口1103之间可以通过总线或信号线相连。各个外围设备可以通过总线、信号线或电路板与外围设备接口1103相连。可选地，外围设备包括：射频电路1104、显示屏1105、摄像头组件1106、音频电路1107、定位组件1108和电源1109中的至少一种。

[0225] 外围设备接口1103可被用于将I/O(Input /Output，输入/输出)相关的至少一个外围设备连接到处理器1101和存储器1102。在一些实施例中，处理器1101、存储器1102和外围设备接口1103被集成在同一芯片或电路板上；在一些其他实施例中，处理器1101、存储器1102和外围设备接口1103中的任意一个或两个可以在单独的芯片或电路板上实现，本实施例对此不加以限定。

[0226] 射频电路1104用于接收和发射RF(Radio Frequency，射频)信号，也称电磁信号。射频电路1104通过电磁信号与通信网络以及其他通信设备进行通信。射频电路1104将电信号转换为电磁信号进行发送，或者，将接收到的电磁信号转换为电信号。可选地，射频电路1104包括：天线系统、RF收发器、一个或多个放大器、调谐器、振荡器、数字信号处理器、编解码芯片组、用户身份模块卡等等。射频电路1104可以通过至少一种无线通信协议来与其它设备进行通信。该无线通信协议包括但不限于：城域网、各代移动通信网络(2G、3G、4G及

5G)、无线局域网和/或WiFi(Wireless Fidelity,无线保真)网络。在一些实施例中,射频电路1104还可以包括NFC(Near Field Communication,近距离无线通信)有关的电路,本申请对此不加以限定。

[0227] 显示屏1105用于显示UI(User Interface,用户界面)。该UI可以包括图形、文本、图标、视频及其它们的任意组合。当显示屏1105是触摸显示屏时,显示屏1105还具有采集在显示屏1105的表面或表面上方的触摸信号的能力。该触摸信号可以作为控制信号输入至处理器1101进行处理。此时,显示屏1105还可以用于提供虚拟按钮和/或虚拟键盘,也称软按钮和/或软键盘。在一些实施例中,显示屏1105可以为一个,设置在终端1100的前面板;在另一些实施例中,显示屏1105可以为至少两个,分别设置在终端1100的不同表面或呈折叠设计;在另一些实施例中,显示屏1105可以是柔性显示屏,设置在终端1100的弯曲表面上或折叠面上。甚至,显示屏1105还可以设置成非矩形的不规则图形,也即异形屏。显示屏1105可以采用LCD(Liquid Crystal Display,液晶显示屏)、OLED(Organic Light-Emitting Diode,有机发光二极管)等材质制备。

[0228] 摄像头组件1106用于采集图像或视频。可选地,摄像头组件1106包括前置摄像头和后置摄像头。前置摄像头设置在终端1100的前面板,后置摄像头设置在终端1100的背面。在一些实施例中,后置摄像头为至少两个,分别为主摄像头、景深摄像头、广角摄像头、长焦摄像头中的任意一种,以实现主摄像头和景深摄像头融合实现背景虚化功能、主摄像头和广角摄像头融合实现全景拍摄以及VR(Virtual Reality,虚拟现实)拍摄功能或者其它融合拍摄功能。在一些实施例中,摄像头组件1106还可以包括闪光灯。闪光灯可以是单色温闪光灯,也可以是双色温闪光灯。双色温闪光灯是指暖光闪光灯和冷光闪光灯的组合,可以用于不同色温下的光线补偿。

[0229] 音频电路1107可以包括麦克风和扬声器。麦克风用于采集用户及环境的声波,并将声波转换为电信号输入至处理器1101进行处理,或者输入至射频电路1104以实现语音通信。出于立体声采集或降噪的目的,麦克风可以为多个,分别设置在终端1100的不同部位。麦克风还可以是阵列麦克风或全向采集型麦克风。扬声器则用于将来自处理器1101或射频电路1104的电信号转换为声波。扬声器可以是传统的薄膜扬声器,也可以是压电陶瓷扬声器。当扬声器是压电陶瓷扬声器时,不仅可以将电信号转换为人类可听见的声波,也可以将电信号转换为人类听不见的声波以进行测距等用途。在一些实施例中,音频电路1107还可以包括耳机插孔。

[0230] 定位组件1108用于定位终端1100的当前地理位置,以实现导航或LBS(Location Based Service,基于位置的服务)。定位组件1108可以是基于美国的GPS(Global Positioning System,全球定位系统)、中国的北斗系统、俄罗斯的格雷纳斯系统或欧盟的伽利略系统的定位组件。

[0231] 电源1109用于为终端1100中的各个组件进行供电。电源1109可以是交流电、直流电、一次性电池或可充电电池。当电源1109包括可充电电池时,该可充电电池可以支持有线充电或无线充电。该可充电电池还可以用于支持快充技术。

[0232] 本领域技术人员可以理解,图11中示出的结构并不构成对终端1100的限定,可以包括比图示更多或更少的组件,或者组合某些组件,或者采用不同的组件布置。

[0233] 可选地,该计算设备提供为服务器。图12是本申请实施例提供的一种服务器的结

构示意图，该服务器1200可因配置或性能不同而产生比较大的差异，可以包括一个或一个以上处理器(Central Processing Units，CPU)1201和一个或一个以上的存储器1202，其中，所述存储器1202中存储有至少一条计算机程序，所述至少一条计算机程序由所述处理器1201加载并执行以实现上述各个方法实施例提供的方法。当然，该服务器还可以具有有线或无线网络接口、键盘以及输入输出接口等部件，以便进行输入输出，该服务器还可以包括其他用于实现设备功能的部件，在此不做赘述。

[0234] 本申请实施例还提供了一种计算机可读存储介质，该计算机可读存储介质中存储有至少一条计算机程序，该至少一条计算机程序由处理器加载并执行，以实现上述实施例的联邦学习方法中所执行的操作。

[0235] 本申请实施例还提供了一种计算机程序产品或计算机程序，计算机程序产品或计算机程序包括计算机程序代码，计算机程序代码存储在计算机可读存储介质中，计算设备的处理器从计算机可读存储介质读取计算机程序代码，处理器执行计算机程序代码，使得计算设备实现如上述实施例的联邦学习方法中所执行的操作。在一些实施例中，本申请实施例所涉及的计算机程序可被部署在一个计算设备上执行，或者在位于一个地点的多个计算设备上执行，又或者，在分布在多个地点且通过通信网络互连的多个计算设备上执行，分布在多个地点且通过通信网络互连的多个计算设备可以组成区块链系统。

[0236] 本领域普通技术人员可以理解实现上述实施例的全部或部分步骤可以通过硬件来完成，也可以通过程序来指令相关的硬件完成，所述的程序可以存储于一种计算机可读存储介质中，上述提到的存储介质可以是只读存储器，磁盘或光盘等。

[0237] 以上所述仅为本申请实施例的可选实施例，并不用以限制本申请实施例，凡在本申请实施例的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本申请的保护范围之内。

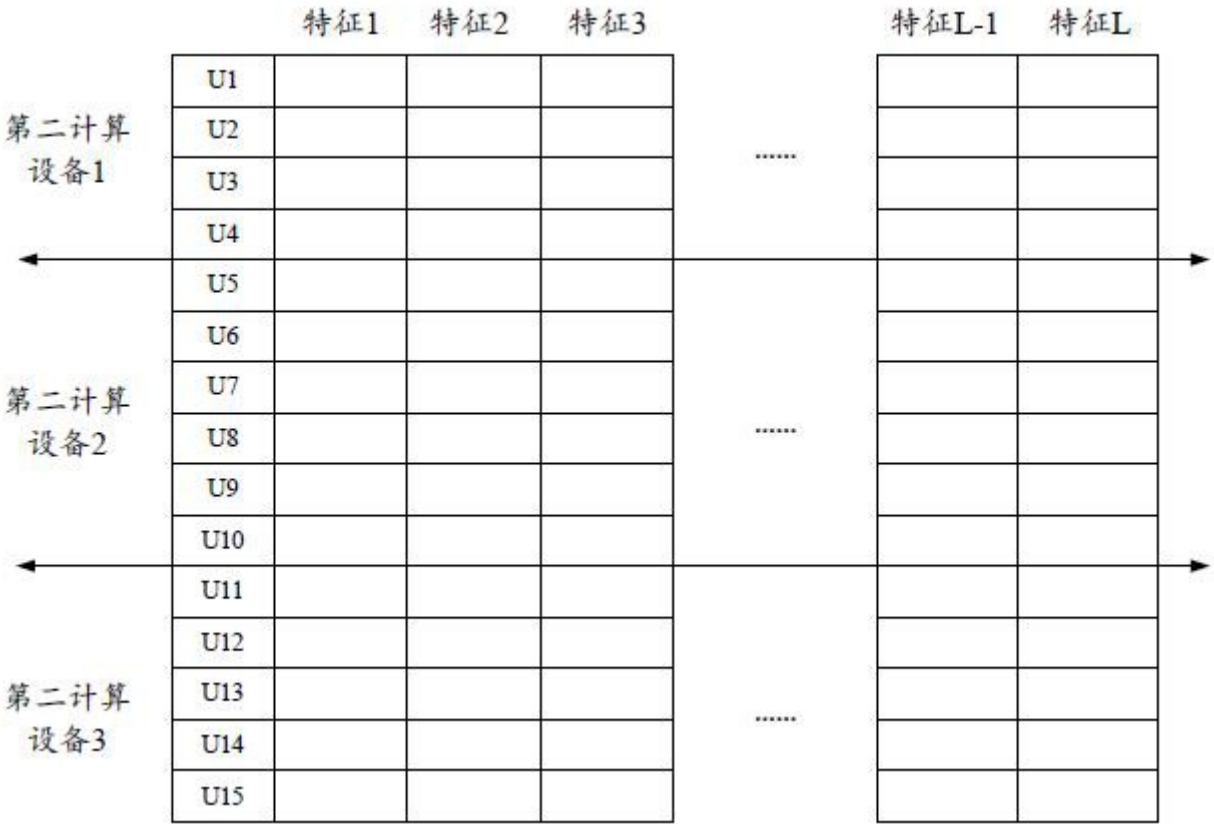

特征1
特征2
特征3
特征L-1
特征L
U1
U2
U3
U4
U5
U6
U7
U8
U9
U10
U11
U12
U13
U14
U15
第二计算设备1
第二计算设备2
第二计算设备3
.....

图1

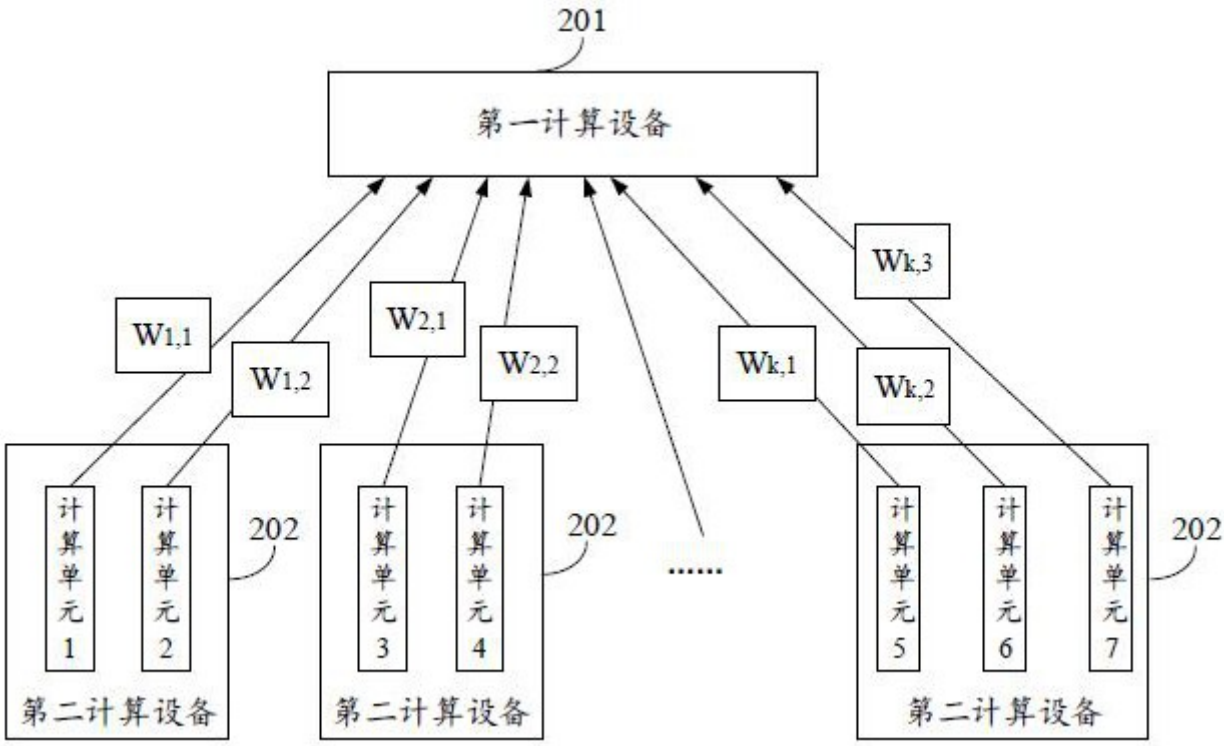

201
第一计算设备
W1,1
W1,2
W2,1
W2,2
Wk,1
Wk,2
Wk,3
计算单元1
计算单元2
计算单元3
计算单元4
计算单元5
计算单元6
计算单元7
202
202
202
第二计算设备
第二计算设备
第二计算设备
.....

图2


第二计算设备
第一计算设备
301、第二计算设备通过本端的多个计算单元组，并行训练联邦学习模型
302、第二计算设备响应于本端的目标计算单元组得到联邦学习模型的本地更新信息，向第一计算设备发送目标计算单元组的本地更新信息
303、第一计算设备接收至少一个第二计算设备发送的本地更新信息，根据接收到的本地更新信息，确定全局更新信息，向至少一个第二计算设备发送全局更新信息
304、第二计算设备接收全局更新信息，根据全局更新信息，更新本端的联邦学习模型

图3

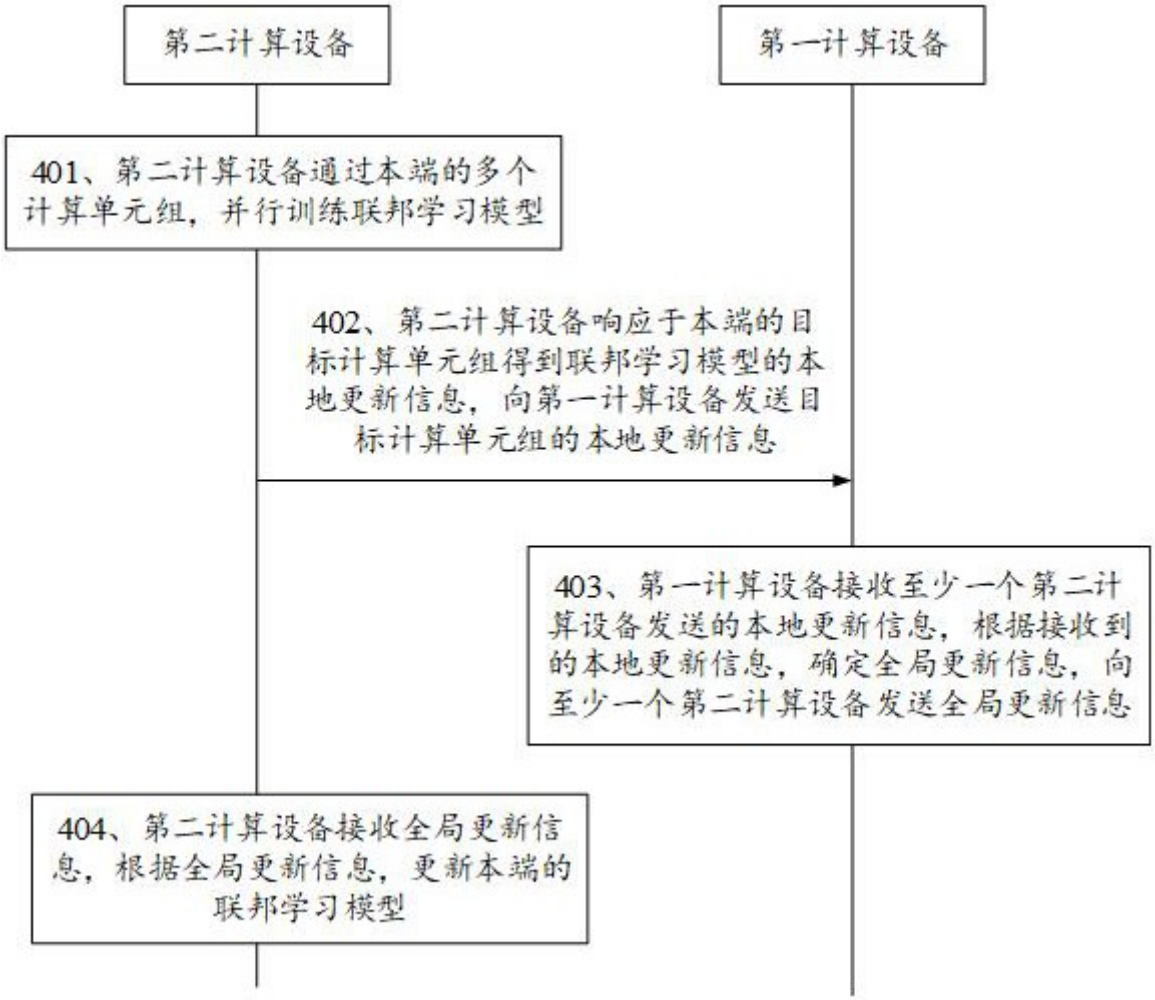

第二计算设备
第一计算设备
401、第二计算设备通过本端的多个计算单元组，并行训练联邦学习模型
402、第二计算设备响应于本端的目标计算单元组得到联邦学习模型的本地更新信息，向第一计算设备发送目标计算单元组的本地更新信息
403、第一计算设备接收至少一个第二计算设备发送的本地更新信息，根据接收到的本地更新信息，确定全局更新信息，向至少一个第二计算设备发送全局更新信息
404、第二计算设备接收全局更新信息，根据全局更新信息，更新本端的联邦学习模型

图4

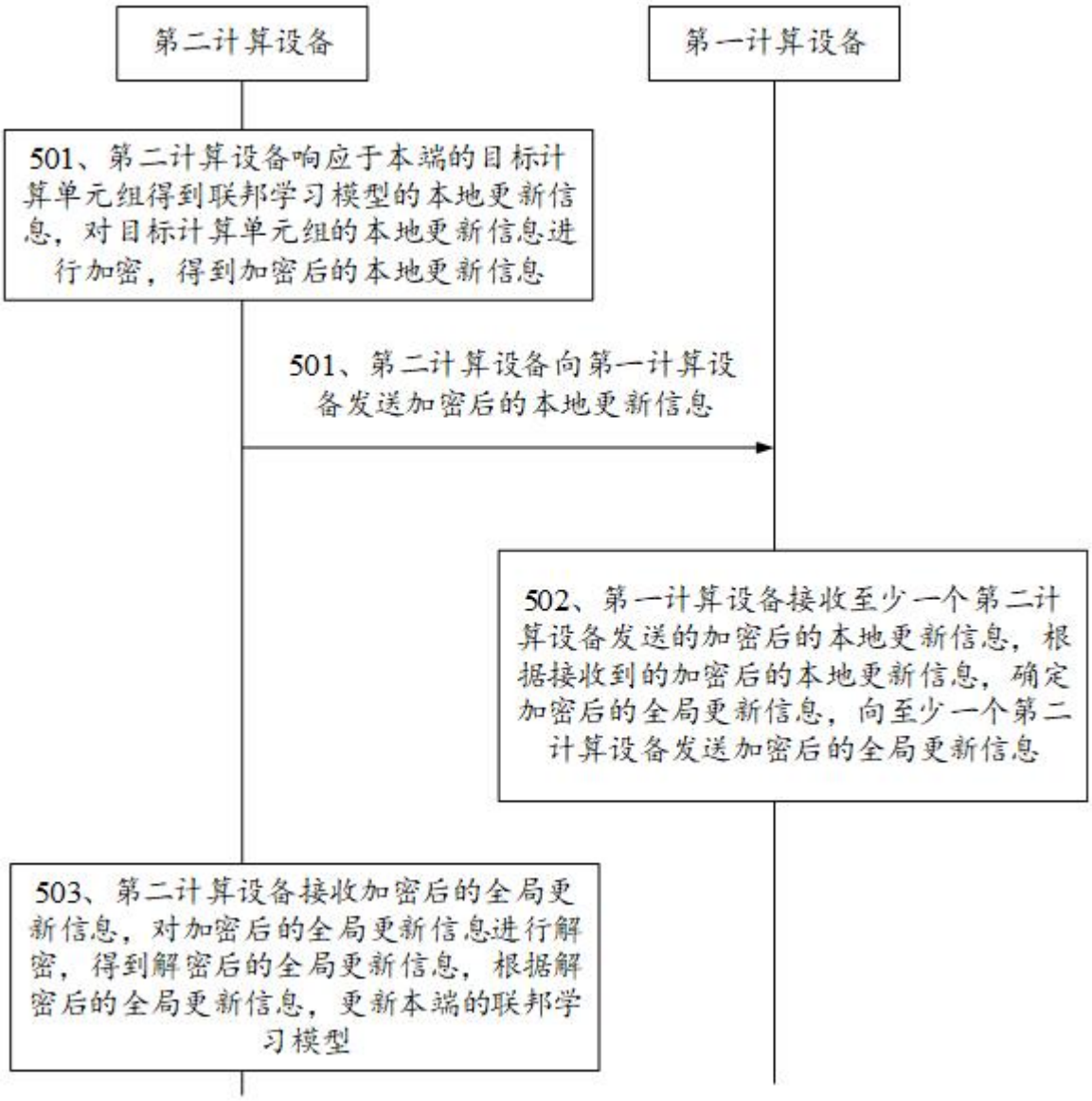

第二计算设备
第一计算设备
501、第二计算设备响应于本端的目标计算单元组得到联邦学习模型的本地更新信息，对目标计算单元组的本地更新信息进行加密，得到加密后的本地更新信息
501、第二计算设备向第一计算设备发送加密后的本地更新信息
502、第一计算设备接收至少一个第二计算设备发送的加密后的本地更新信息，根据接收到的加密后的本地更新信息，确定加密后的全局更新信息，向至少一个第二计算设备发送加密后的全局更新信息
503、第二计算设备接收加密后的全局更新信息，对加密后的全局更新信息进行解密，得到解密后的全局更新信息，根据解密后的全局更新信息，更新本端的联邦学习模型

图5

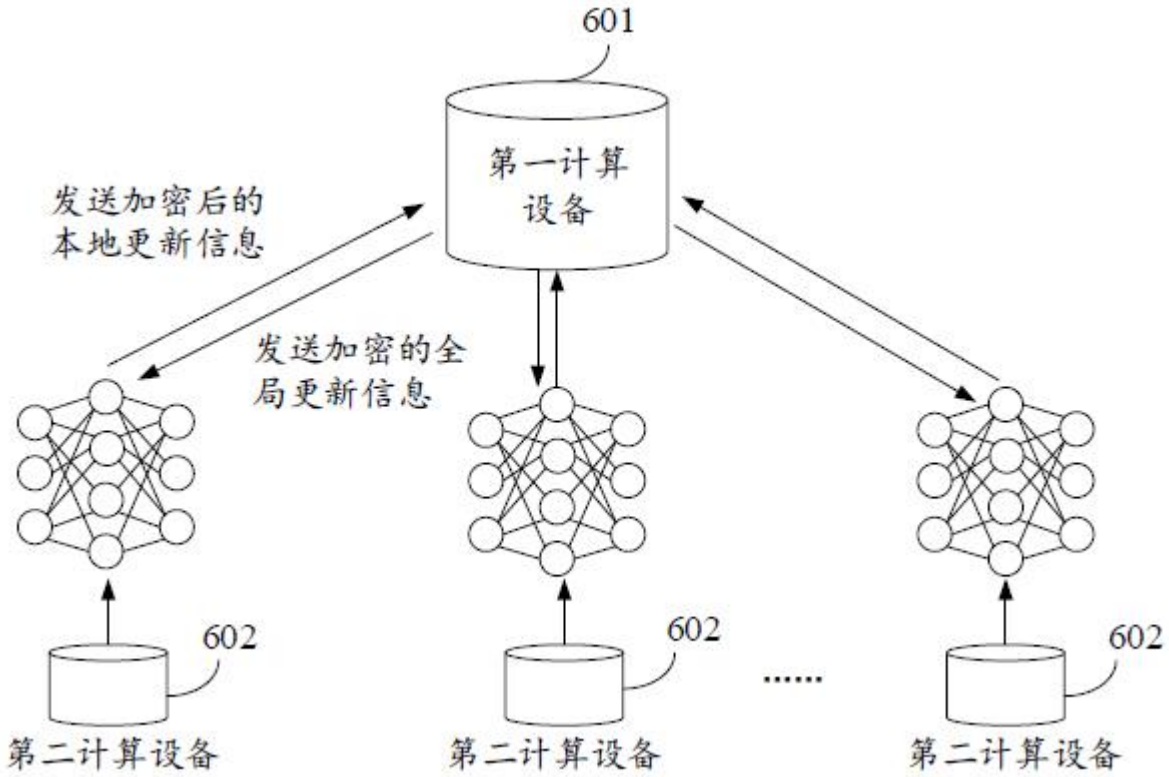

601
第一计算设备
发送加密后的本地更新信息
发送加密的全局更新信息
602
602
602
.....
第二计算设备
第二计算设备
第二计算设备

图6

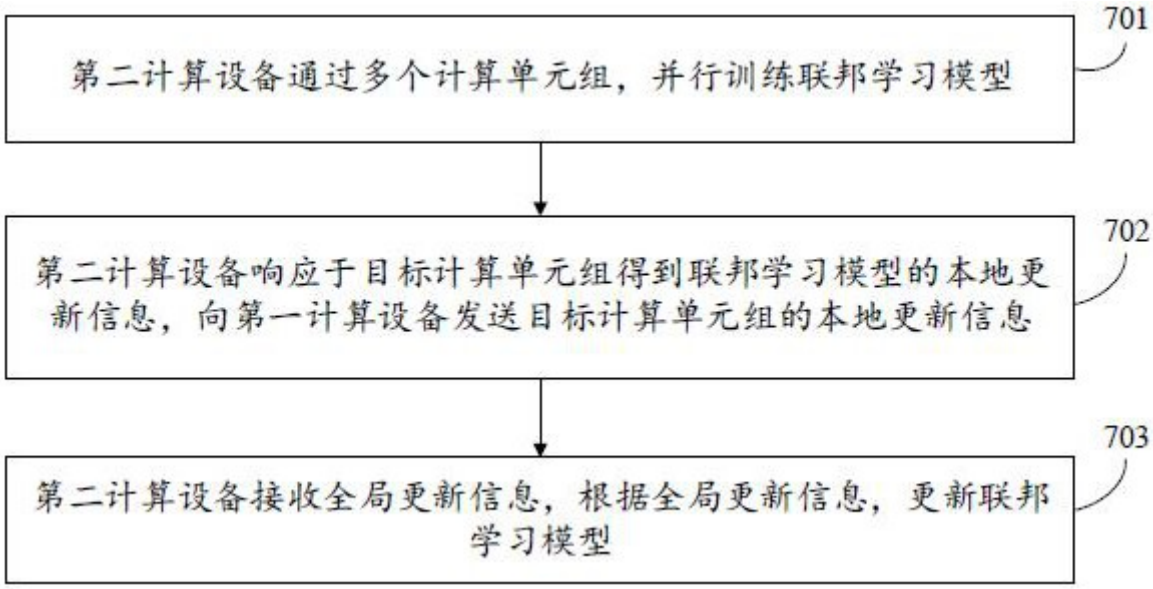

701
第二计算设备通过多个计算单元组，并行训练联邦学习模型
702
第二计算设备响应于目标计算单元组得到联邦学习模型的本地更新信息，向第一计算设备发送目标计算单元组的本地更新信息
703
第二计算设备接收全局更新信息，根据全局更新信息，更新联邦学习模型

图7

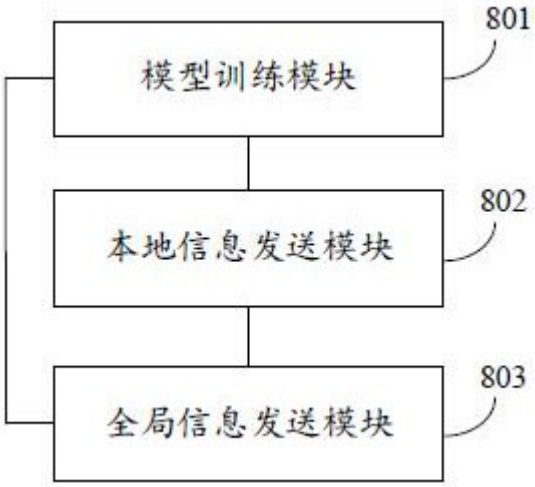

801
模型训练模块
802
本地信息发送模块
803
全局信息发送模块

图8

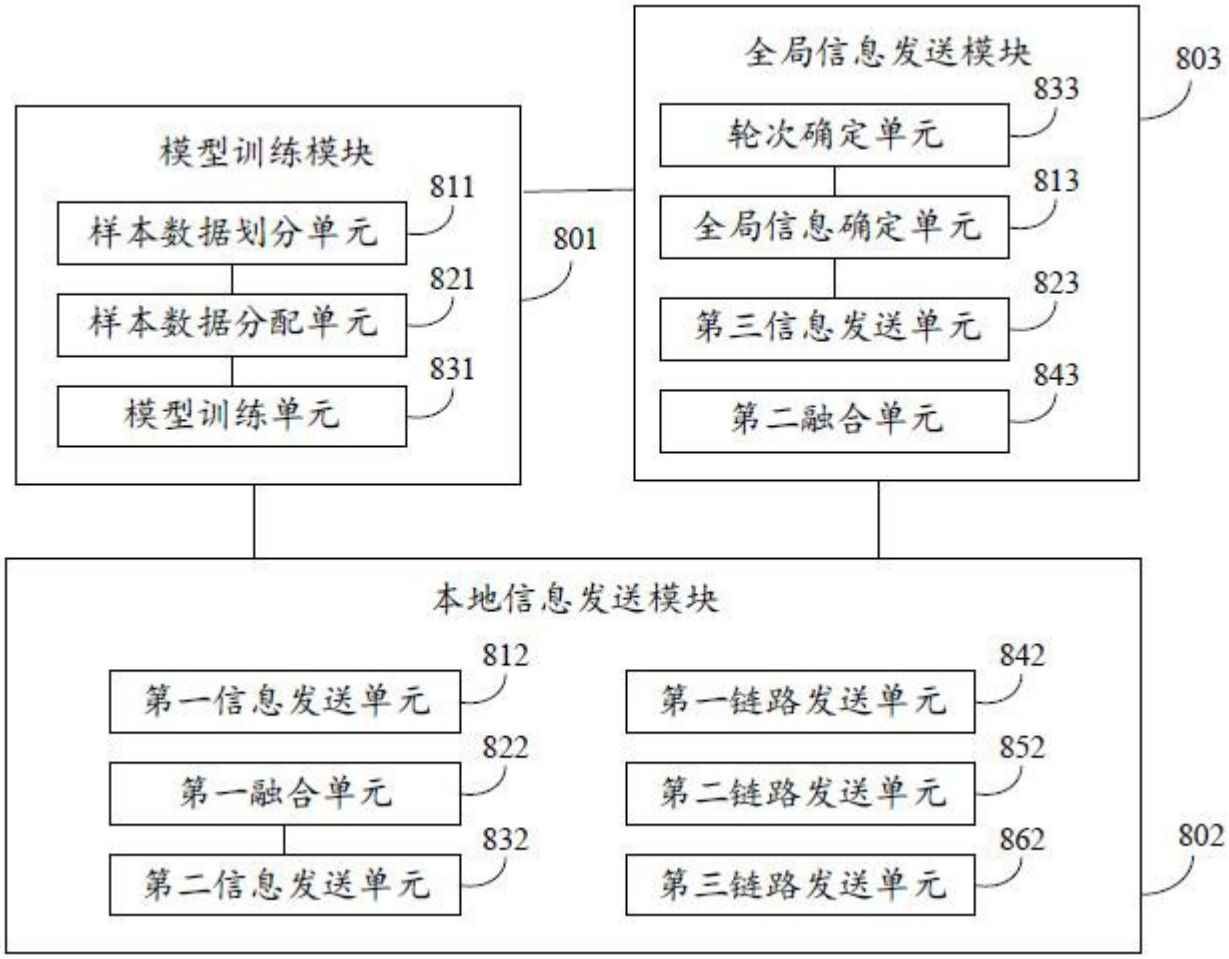

全局信息发送模块
803
833
轮次确定单元
813
全局信息确定单元
823
第三信息发送单元
843
第二融合单元
模型训练模块
811
样本数据划分单元
821
样本数据分配单元
831
模型训练单元
801
本地信息发送模块
812
第一信息发送单元
822
第一融合单元
832
第二信息发送单元
842
第一链路发送单元
852
第二链路发送单元
862
第三链路发送单元
802

图9


1001
模型训练模块
1002
本地信息发送模块

图10

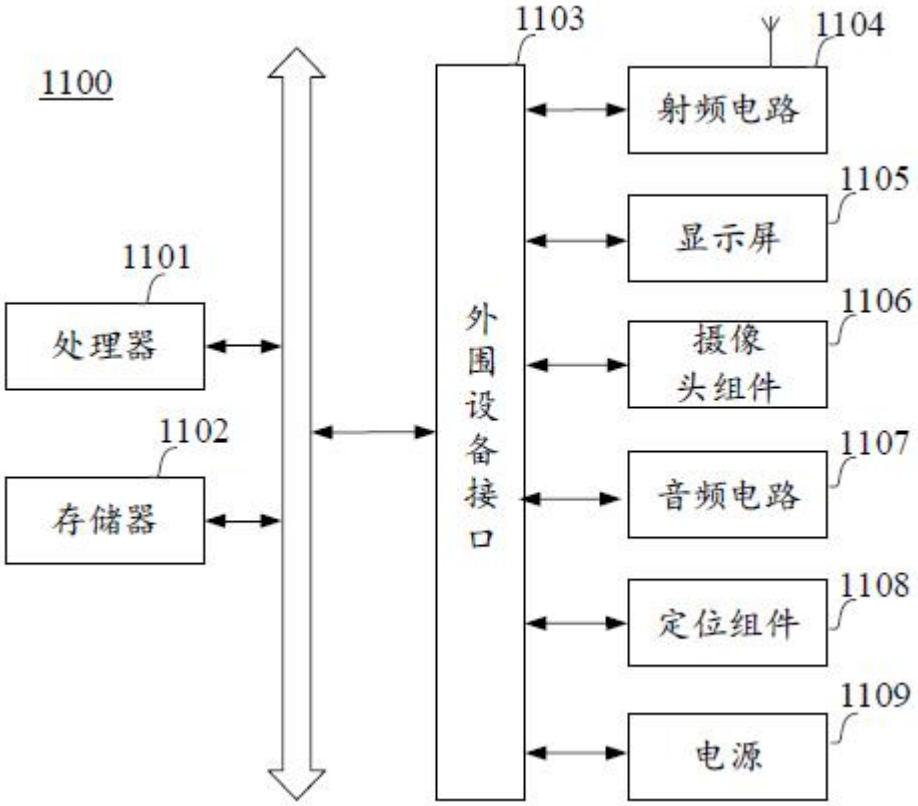

1100
1101
处理器
1102
存储器
1103
外围设备接口
1104
射频电路
1105
显示屏
1106
摄像头组件
1107
音频电路
1108
定位组件
1109
电源

图11

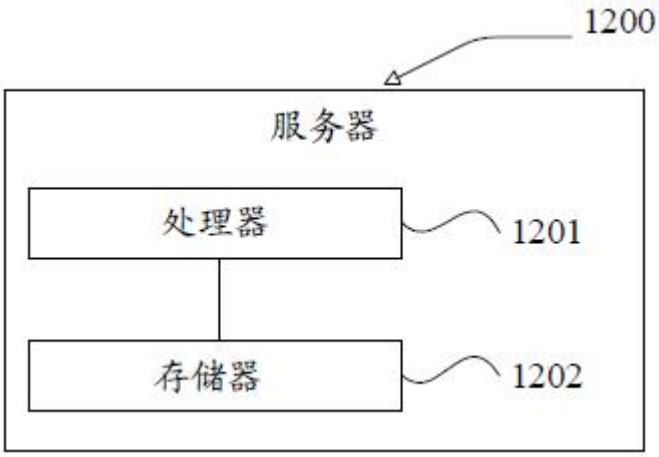


图12