

一种训练模型的方法、数据处理的方法以及装置

本申请要求于 2020 年 12 月 04 日提交中国专利局、申请号为 202011401668.9、申请名称为“一种训练模型的方法、数据处理的方法以及装置”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

5

技术领域

本申请涉及人工智能技术领域，具体涉及一种训练模型的方法、数据处理的方法以及装置。

10 背景技术

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分支，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作出反应的智能机器。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。人工智能领域的研究包括机器人，自然语言处理，计算机视觉，决策与推理，人机交互，推荐与搜索，AI 基础理论等。

随着人工智能的发展，联邦学习逐渐成为发展趋势，联邦学习是指一种机器学习系统，能有效帮助多个端侧设备在满足数据隐私保护的要求下，联合训练模型。在联邦学习中，如何提升端侧设备训练得到的模型的性能，成为亟待解决的技术问题。

20 发明内容

本申请实施例提供一种训练模型的方法、数据处理的方法以及装置，在联邦学习中，提升端侧设备训练得到的模型的性能。

为达到上述目的，本申请实施例提供如下技术方案：

25 本申请第一方面提供一种训练模型的方法，该方法适用于机器学习系统，机器学习系统可以包括服务器和至少两个端侧设备，其中，该机器学习系统可以是联邦学习系统。针对第一端侧设备，第一端侧设备是至少两个端侧中的任意一个端侧设备，该方法可以包括：接收服务器发送的第一共享模型。其中，接收服务器发送的第一共享模型可以理解为接收服务器发送的第一共享模型的全部参数或者部分参数。通过所述第一共享模型输出针对数据集的第一预测结果。本申请有时也将数据集称为训练数据集，二者表示相同的意思，用于表示端侧设备本地存储的数据集。根据所述第一预测结果获取第一损失值，比如可以将数据集输入到第一共享模型中，以输出数据集的第一预测结果。以第二共享模型用于执行分类任务为例进行说明，第一端侧设备可以获取样本数据集，样本数据集包括多个样本，多个样本中的每个样本均包括第一标签。可以用第二共享模型对数据集进行分类，得到测试数据集中的每个样本的第二标签，可以将第一预测结果理解为第二标签。第一损失值用于表示第一标签和第二标签的差异。通过所述第一端侧设备的第一私有模型输出针对所述数据集的第二预测结果；根据所述第二预测结果获取第二损失值。对第一损失值和第二损失值进行第二融合处理，以获取第三损失值，第三损失值用于更新私有模型。由第一方面

30

35

可知，本申请提供的方案在端侧设备上训练两个模型，一个模型参与联邦学习和融合的过程，一个模型不直接参与联邦学习和融合的过程，根据训练后的两个模型分别获取两个模型的损失值，对两个模型的损失值进行融合，并通过融合后的损失值更新私有模型。机器学习系统中的各个端侧设备的数据分布往往是非独立同分布（non-independent and identically, Non-IID）的，数据分布之间存在较大差异，其中，数据分布不同可以理解为同一个标签在不同客户端的数据集中的比例不同。因此，如果仅采用第二损失值更新第一私有模型，训练后的第一私有模型对于全局数据的预测性能不尽如人意，其中，可以将全局数据理解为包括第一端侧设备的本地数据和该至少两个端侧设备的数据的集合。本申请提供的方案由于服务器融合了多个端侧设备发送的共享模型，并将该融合后的共享模型发送至各个端侧模型，通过该共享模型输出的预测结果确定的损失值（第一损失值）的可信度更高，用该可信度更高的损失值和私有模型的损失值（第二损失值）进行融合处理，并通过融合处理后的损失值（第三损失值）更新私有模型，指导私有模型的训练过程，使私有模型不仅对本地数据有良好的预测结果，对于全局数据也有良好的预测结果。换句话说，本申请提供的方案通过实现两个模型之间的信息传递，使端侧设备训练得到的私有模型性能更优。

可选地，结合上述第一方面，在第一种可能的实施方式中，所述第三损失值还用于更新所述第一共享模型，以得到第二共享模型，所述方法还包括：向所述服务器发送所述第二共享模型，所述第二共享模型用于所述服务器更新所述第一共享模型。由第一方面第一种可能的实施方式可知，根据训练后的两个模型分别获取两个模型的损失值，对两个模型的损失值进行融合，并通过融合后的损失值更新共享模型，实现两个模型之间的信息传递，以使端侧设备训练得到的共享模型性能更优。

可选地，结合上述第一方面或第一方面第一种可能的实施方式，在第二种可能的实施方式中，第一损失值可以包括交叉熵损失值和双向蒸馏损失值中的一个或者多个，第二损失值可以包括交叉熵损失值和双向蒸馏损失值中的一个或者多个。由第一方面第二种可能的实施方式可知，给出了几种典型的第一损失值和第二损失值，增加方案的多样性，需要说明的是，本申请中获取第一损失值包括但不限于交叉熵损失值和双向蒸馏损失值，第二损失值包括但不限于交叉熵损失值和双向蒸馏损失值。

可选地，结合上述第一方面或第一方面第一种至第一方面第二种可能的实施方式，在第三种可能的实施方式中，所述训练数据集包括需要隐私保护的第一训练数据集和不需要隐私保护的第二训练数据集，所述通过所述第一共享模型输出针对训练数据集的第一预测结果，包括：通过所述第一共享模型输出针对所述第二训练数据集的第一预测结果；所述通过所述第一端侧设备的第一私有模型输出针对所述训练数据集的第二预测结果，包括：通过所述第一端侧设备的第一私有模型输出针对所述第一训练数据集和第二训练数据集的第二预测结果。由第一方面第三种可能的实施方式可知，在一些可能的应用场景中，端侧设备可能对数据的隐私保护有很高的需求，则可以对端侧设备的训练数据按照需要隐私保护的高低进行划分，其中对隐私保护要求高的数据仅参与私有模型的训练过程，其余的数据可以既参与共享模型的训练过程也参与私有模型的训练过程。

可选地，结合上述第一方面或第一方面第一种至第一方面第三种可能的实施方式，在第四种可能的实施方式中，对第一损失值和第二损失值进行第二融合处理，以获取第三损失值，可以包括：对第一损失值和第二损失值进行加权处理，以获取第三损失值。由第一方面第五种可能的实施方式可知，给出了一种具体的对第一损失值和第二损失值进行融合处理的方式，增加了方案的多样性。

可选地，结合上述第一方面第五种可能的实施方式，在第五种可能的实施方式中，对第一损失值和第二损失值进行加权处理，以获取第三损失值，可以包括：对第一损失值和第二损失值进行求平均值处理，以获取第三损失值。由第一方面第六种可能的实施方式可知，给出了一种具体的对第一损失值和第二损失值进行融合处理的方式，增加了方案的多样性。

可选地，结合上述第一方面或第一方面第一种至第一方面第五种可能的实施方式，在第六种可能的实施方式中，第一共享模型和第一私有模型共享特征提取模型。在一种可能的实施方式中，接收第一共享模型之前，第一终端设备存储有第二私有模型，该方法还包括：根据第一共享模型的特征提取模型更新第二私有模型的特征提取模型，以得到第一私有模型，第一私有模型还用于替换第二私有模型。在另一种可能的实施方式中，第一私有模型直接采用第一共享模型的特征提取模型。由第一方面第六种可能的实施方式可知，端侧设备训练的共享模型和私有模型可以采用相同的特征提取模型，端侧设备训练的共享模型和私有模型可以采用相同的任务模型或者采用不同的任务任务模型，共享模型和私有模型采用相同的特征提取模型，有利于后续的融合处理过程。

可选地，结合上述第一方面或第一方面第一种至第一方面第六种可能的实施方式，在第七种可能的实施方式中，向服务器发送第三共享模型，其中，第一端侧设备向服务器发送第三共享模型可以理解为第一端侧设备向服务器发送第三共享模型的全部权重参数。或者第一端侧设备向服务器发送第三共享模型可以理解为第一端侧设备向服务器发送第三共享模型的部分权重参数，比如，如果第三共享模型是第一端侧设备对初始的共享模型训练到一定程度获取的，其中部分权重参数是指第三共享模型和初始的共享模型不同的权重参数。以使服务器对至少两个端侧发送的第三共享模型进行第一融合处理，以获取第三共享模型。服务器可以采用多种融合算法对接收到的多个第三共享模型进行融合处理，以获取第三共享模型。比如可以对多个第三共享模型求平均值以获取第三共享模型，或者可以对多个第三共享模型进行加权处理，以获取第一共享模型，或者可以采用其他预设的算法那对多个第一共享模型进行处理，以获取第一共享模型。

本申请第二方面提供一种数据处理的方法，该方法适用于机器学习系统，该机器学习系统可以包括服务器和至少两个端侧设备，针对第一端侧设备，第一端侧设备是至少两个端侧中的任意一个端侧设备，该方法可以包括：获取待处理数据。根据端侧设备存储的目标模型对待处理数据进行处理，以获取预测结果，其中，所述目标模型是通过第三损失值更新第一私有模型获取的，所述第三损失值是对第一损失值和第二损失值进行融合处理后获取的，所述第一损失值是通过第一预测结果获取的，所述第一预测结果是第一共享模型输出的针对训练数据集的预测结果，所述第一共享模型是从服务器中获取的，所述第二损

失值是通过第二预测结果获取的, 所述第二预测结果是第一私有模型输出的针对训练数据集的预测结果。第一共享模型由第二方面可知, 本申请提供的方案, 目标模型是通过共享模型学习到的知识以及本地训练数据集训练得到的模型, 相比于现有技术中端侧设备训练得到的模型, 本申请中的目标模型性能更优。

5 可选地, 结合上述第二方面, 在第一种可能的实施方式中, 所述第三损失值还用于更新所述第一共享模型, 以得到第二共享模型, 所述第二共享模型用于发送至所述服务器, 以使所述服务器更新所述第一共享模型。由第二方面第一种可能的实施方式可知, 根据训练后的两个模型分别获取两个模型的损失值, 对两个模型的损失值进行融合, 并通过融合后的损失值更新共享模型, 实现两个模型之间的信息传递, 以使端侧设备训练得到的共享模型性能更优。

10 可选地, 结合上述第二方面或第二方面第一种可能的实施方式, 在第二种可能的实施方式中, 所述第一损失值包括交叉熵损失值和双向蒸馏损失值中的一个或者多个, 所述第二损失值包括交叉熵损失值和双向蒸馏损失值中的一个或者多个。由第二方面第二种可能的实施方式可知, 给出了几种典型的第一损失值和第二损失值, 增加方案的多样性。

15 可选地, 结合上述第二方面或第二方面第一种至第二方面第二种可能的实施方式, 在第三种可能的实施方式中, 所述训练数据集包括第一训练数据集和第二训练数据集, 所述第一训练数据集预先设定需要隐私保护, 所述第二训练数据集预先设定不需要隐私保护, 所述第一预测结果是所述第一共享模型输出的针对所述第二训练数据集的预测结果, 所述第二预测结果是所述第一私有模型输出的针对所述第一训练数据集和所述第二训练数据集的预测结果。由第二方面第三种可能的实施方式可知, 在一些可能的应用场景中, 端侧设备可能对数据的隐私保护有很高的需求, 则可以对端侧设备的训练数据按照需要隐私保护的高低进行划分, 其中对隐私保护要求高的数据仅参与私有模型的训练过程, 其余的数据可以既参与共享模型的训练过程也参与私有模型的训练过程。

20 可选地, 结合上述第二方面或第二方面第一种至第二方面第三种可能的实施方式, 在第四种可能的实施方式中, 所述第三损失值是通过将所述第一损失值和所述第二损失值进行加权处理后获取的。由第二方面第四种可能的实施方式可知, 给出了一种具体的对第一损失值和第二损失值进行融合处理的方式, 增加了方案的多样性。

25 可选地, 结合上述第二方面第五种可能的实施方式, 在第五种可能的实施方式中, 所述第三损失值具体是通过将所述第一损失值和所述第二损失值进行求平均值处理后获取的。由第二方面第五种可能的实施方式可知, 给出了一种具体的对第一损失值和第二损失值进行融合处理的方式, 增加了方案的多样性。

30 可选地, 结合上述第二方面或第二方面第一种至第二方面第五种可能的实施方式, 在第六种可能的实施方式中, 接收所述第一共享模型之前, 所述第一终端设备存储有第二私有模型, 所述第一私有模型是根据所述第一共享模型的特征提取模型更新所述第二私有模型的特征提取模型后获取的, 所述第一私有模型还用于替换所述第二私有模型。

35 可选地, 结合上述第二方面, 在第七种可能的实施方式中, 待处理数据是需要隐私保护的数据时, 通过所述端侧设备存储的目标模型对该待处理数据进行处理, 以获取预测结

果。该待处理数据是不需要隐私保护的数据时，既可以通过端侧设备存储的目标模型对该待处理数据进行处理，也可以通过第二共享模型对该待处理数据进行处理。第二共享模型是通过第三损失值更新第一共享模型后获取的模型。

本申请第三方面提供一种端侧设备，端侧设备适用于机器学习系统，该机器学习系统
5 可以包括服务器和至少两个端侧设备，针对第一端侧设备，第一端侧设备是至少两个端侧
中的任意一个端侧设备，可以包括收发模块和训练模块所述收发模块，用于：第一共享模
型所述收发模块，还用于接收所述服务器发送的所述第一共享模型；所述训练模块，用于：
通过所述第一共享模型输出针对训练数据集的第一预测结果；根据所述第一预测结果获取
10 第一损失值；通过所述第一端侧设备的第一私有模型输出针对所述训练数据集的第二预测
结果；根据所述第二预测结果获取第二损失值；对所述第一损失值和所述第二损失值进行
第二融合处理，以获取第三损失值，所述第三损失值用于更新所述第一私有模型。

可选地，结合上述第三方面，在第一种可能的实施方式中，所述第三损失值还用于更
新所述第一共享模型，以得到第二共享模型，所述收发模块，还用于：向所述服务器发送
15 所述第二共享模型，所述第二共享模型用于所述服务器更新所述第一共享模型。

可选地，结合上述第三方面或第三方面第一种可能的实施方式，在第二种可能的实施
20 方式中，所述第一损失值包括交叉熵损失值和双向蒸馏损失值中的一个或者多个，所述第
二损失值包括交叉熵损失值和双向蒸馏损失值中的一个或者多个。

可选地，结合上述第三方面或第三方面第一种至第三方面第二种可能的实施方式，在
第三种可能的实施方式中，所述训练数据集包括第一训练数据集和第二训练数据集，所述
25 第一训练数据集预先设定需要隐私保护，所述第二训练数据集预先设定不需要隐私保护，
所述训练模块，具体用于通过所述第一共享模型输出所述第二训练数据集的第一预测结果；
所述训练模块，具体用于通过所述第一端侧设备的第一私有模型输出所述第一训练数据集
和第二训练数据集的第二预测结果。

可选地，结合上述第三方面或第三方面第一种至第三方面第三种可能的实施方式，在
第四种可能的实施方式中，所述训练模块具体用于：对所述第一损失值和所述第二损失值
25 进行加权处理，以获取所述第三损失值。

可选地，结合上述第三方面第五种可能的实施方式，在第五种可能的实施方式中，所
述训练模块具体用于：对所述第一损失值和所述第二损失值进行求平均值处理，以获取所
述第三损失值。

可选地，结合上述第三方面或第三方面第一种至第三方面第五种可能的实施方式，在
第六种可能的实施方式中，接收所述第一共享模型之前，所述第一终端设备存储有第二私
30 有模型，所述训练模块还用于：根据所述第一共享模型的特征提取模型更新所述第二私有
模型的特征提取模型，以得到所述第一私有模型，所述第一私有模型还用于替换所述第二
私有模型。

可选地，结合上述第三方面或第三方面第一种至第三方面第六种可能的实施方式，在
第七种可能的实施方式，所述第一端侧还用于：向服务器发送第二共享模型，以使所述服
35 务器对所述至少两个端侧发送的所述第二共享模型进行第一融合处理，以获取第一共享模

型。

第三方面以及第三方面各个实施方式的有益效果可以参照第一方面以及第一方面各个实施方式的有益效果进行理解，这里不再重复赘述。

本申请第四方面提供一种端侧设备，端侧设备适用于机器学习系统，该机器学习系统
5 可以包括服务器和至少两个端侧设备，针对第一端侧设备，第一端侧设备是至少两个端侧
中的任意一个端侧设备，可以包括：获取模块，用于获取待处理数据。推理模块，用于根
据端侧设备存储的目标模型对待处理数据进行处理，以获取预测结果，所述目标模型是通
过第三损失值更新第一私有模型获取的，所述第三损失值是对第一损失值和第二损失值进
10 行融合处理后获取的，所述第一损失值是通过第一预测结果获取的，所述第一预测结果
是第一共享模型输出的针对训练数据集的预测结果，所述第一共享模型是从服务器中获取
的，所述第二损失值是通过第二预测结果获取的，所述第二预测结果是第一私有模型输出
的针对训练数据集的预测结果。

可选地，结合上述第四方面，在第一种可能的实施方式中，所述第三损失值还用于更
新所述第一共享模型，以得到第二共享模型，所述第二共享模型用于发送至所述服务器，
15 以使所述服务器更新所述第一共享模型。

可选地，结合上述第四方面或第四方面第一种可能的实施方式，在第二种可能的实
施方式中，所述第一损失值包括交叉熵损失值和双向蒸馏损失值中的一个或者多个，所述第
二损失值包括交叉熵损失值和双向蒸馏损失值中的一个或者多个。

可选地，结合上述第四方面或第四方面第一种至第四方面第二种可能的实施方式，在
20 第三种可能的实施方式中，所述训练数据集包括需要隐私保护的第一训练数据集和不需要
隐私保护的所述第二训练数据集，所述第一预测结果是所述第一共享模型输出的针对所述第
二训练数据集的预测结果，所述第二预测结果是所述第一私有模型输出的针对所述第一训
练数据集和所述第二训练数据集的预测结果。

可选地，结合上述第四方面或第四方面第一种至第四方面第三种可能的实施方式，在
25 第四种可能的实施方式中，所述第三损失值是通过所述对所述第一损失值和所述第二损失值
进行加权处理后获取的。

可选地，结合上述第四方面第五种可能的实施方式，在第五种可能的实施方式中，所
述第三损失值具体是通过所述对所述第一损失值和所述第二损失值进行求平均值处理后获
取的。

30 可选地，结合上述第四方面或第四方面第一种至第四方面第五种可能的实施方式，在
第六种可能的实施方式中，接收所述第一共享模型之前，所述第一终端设备存储有第二私
有模型，所述第一私有模型是根据所述第一共享模型的特征提取模型更新所述第二私有模
型的特征提取模型后获取的，所述第一私有模型还用于替换所述第二私有模型。

第四方面以及第四方面各个实施方式的有益效果可以参照第二方面以及第二方面各个
35 实施方式的有益效果进行理解，这里不再重复赘述。

本申请第五方面提供一种机器学习系统，该机器学习系统可以包括服务器和至少两个
端侧设备，第一端侧设备是至少两个端侧中的任意一个端侧设备，述服务器，用于向所述

第一端侧设备发送第一共享模型；所述第一端侧设备，用于：通过所述第一共享模型输出针对训练数据集的第一预测结果；根据所述第一预测结果获取第一损失值；通过所述第一端侧设备的第一私有模型输出针对所述训练数据集的第二预测结果；根据所述第二预测结果获取第二损失值；对第一损失值和第二损失值进行第二融合处理，以获取第三损失值，第三损失值用于更新私有模型。

可选地，结合上述第五方面，在第一种可能的实施方式中，所述第三损失值还用于更新所述第一共享模型，以得到第二共享模型，第一端侧设备，还用于：向所述服务器发送所述第二共享模型，服务器，还用于根据第二共享模型更新所述第一共享模型。

可选地，结合上述第五方面或第五方面第一种可能的实施方式，在第二种可能的实施方式中，第一损失值可以包括交叉熵损失值和双向蒸馏损失值中的一个或者多个，第二损失值可以包括交叉熵损失值和双向蒸馏损失值中的一个或者多个。

可选地，结合上述第五方面或第五方面第一种至第五方面第二种可能的实施方式，在第三种可能的实施方式中，所述训练数据集包括需要隐私保护的第一训练数据集和不需要隐私保护的第二训练数据集，第一终端设备，具体用于通过所述第一共享模型输出所述第二训练数据集的第一预测结果；第一终端设备，具体用于通过所述第一端侧设备的第一私有模型输出所述第一训练数据集和第二训练数据集的第二预测结果。

可选地，结合上述第五方面或第五方面第一种至第五方面第三种可能的实施方式，在第四种可能的实施方式中，第一终端设备，具体用于对第一损失值和第二损失值进行加权处理，以获取第三损失值。

可选地，结合上述第五方面第五种可能的实施方式，在第五种可能的实施方式中，第一终端设备，具体用于对第一损失值和第二损失值进行求平均值处理，以获取第三损失值。

可选地，结合上述第五方面或第五方面第一种至第五方面第五种可能的实施方式，在第六种可能的实施方式中，接收所述第一共享模型之前，所述第一终端设备存储有第二私有模型，第一终端设备，还用于根据所述第一共享模型的特征提取模型更新所述第二私有模型的特征提取模型，以得到所述第一私有模型，所述第一私有模型还用于替换所述第二私有模型。

可选地，结合上述第五方面或第五方面第一种至第五方面第六种可能的实施方式，在第七种可能的实施方式中，第一端侧设备，还用于向服务器发送第一共享模型。服务器，用于对至少两个端侧发送的第一共享模型进行第一融合处理，以获取第一共享模型。

本申请第六方面提供一种端侧设备，可以包括：存储器，用于存储计算机可读指令。还可以包括，与存储器耦合的处理器，用于执行存储器中的计算机可读指令从而执行如第一方面或第一方面任意一种可能的实施方式所描述的方法。

本申请第七方面提供一种端侧设备，可以包括：存储器，用于存储计算机可读指令。还可以包括，与存储器耦合的处理器，用于执行存储器中的计算机可读指令从而执行如第二方面或第二方面任意一种可能的实施方式所描述的方法。

本申请第八方面提供一种计算机可读存储介质，计算机可读存储介质中存储有指令，当指令在计算机装置上运行时，使得计算机装置执行如第一方面或第一方面任意一种可能

的实施方式所描述的方法。

本申请第九方面提供一种计算机可读存储介质，计算机可读存储介质中存储有指令，当指令在计算机装置上运行时，使得计算机装置执行如第二方面或第二方面任意一种可能的实施方式所描述的方法。

5 本申请第十方面提供一种计算机程序产品，当计算机程序产品在计算机上运行时，使得计算机可以执行如第一方面或第一方面任意一种可能的实施方式所描述的方法。

本申请第十一方面提供一种计算机程序产品，当计算机程序产品在计算机上运行时，使得计算机可以执行如第二方面或第二方面任意一种可能的实施方式所描述的方法。

10 本申请第十二方面提供一种芯片，芯片与存储器耦合，用于执行存储器中存储的程序，以执行如第一方面或第一方面任意一种可能的实施方式所描述的方法。

本申请第十三方面提供一种芯片，芯片与存储器耦合，用于执行存储器中存储的程序，以执行如第二方面或第二方面任意一种可能的实施方式所描述的方法。

15 本申请提供的方案在端侧设备上训练两个模型，一个模型参与联邦学习和融合的过程，一个模型不直接参与联邦学习和融合的过程，根据训练后的两个模型分别获取两个模型的损失值，对两个模型的损失值进行融合，并通过融合后的损失值更新该两个模型，实现两个模型之间的信息传递，以使端侧设备训练得到的私有模型性能更优。此外通过本申请提供的方案，也可以解决由于端侧设备的训练数据集的训练样本的数据较少时，可能会出现私有模型过拟合的问题。

附图说明

20 图1为本发明实施例提供的一种人工智能主体框架示意图；
图2为本发明实施例提供的一种应用环境示意图；
图3为本发明实施例提供的一种卷积神经网络结构示意图；
图4为本发明实施例提供的一种卷积神经网络结构示意图；
图5为一种联邦学习系统的架构示意图；
25 图6为一种适用于联邦学习系统的模型训练方法的流程示意图；
图7为本申请实施例提供的一种联邦学习系统的架构示意图；
图8为本申请实施例提供的一种训练模型的方法的流程示意图；
图8-a为本申请实施例提供的另一种联邦学习系统的架构示意图；
图9为本申请实施例提供的一种训练模型的方法的流程示意图；
30 图10为本申请提供的一种数据处理方法的流程示意图；
图11为本申请实施例提供的端侧设备的硬件结构示意图；
图12为本申请实施例提供方案的一种可能的应用场景示意图；
图13为本申请实施例提供的端侧设备的结构示意图；
图14为本申请实施例提供的另一种端侧设备的结构示意图；
35 图15为本申请实施例提供的芯片的一种结构示意图。

具体实施方式

下面结合附图，对本申请的实施例进行描述，显然，所描述的实施例仅仅是本申请一

部分的实施例，而不是全部的实施例。本领域普通技术人员可知，随着技术的发展和场景的出现，本申请实施例提供的技术方案对于类似的技术问题，同样适用。

本申请提供一种训练模型的方法，该方法适用于联邦学习系统。针对目前联邦学习系统中，端侧设备训练获得的模型性能低下的问题，本申请提供的方案通过在端侧设备训练共享模型和私有模型。其中，共享模型参与联邦学习，私有模型不直接参与联邦学习。通过训练后的共享模型获取第一损失值，通过训练后的私有模型获取第二损失值，对第一损失值和第二损失值进行融合处理后获得第三损失值。本申请提供的方案通过第三损失值更新私有模型，以提升端侧设备训练获得的私有模型的性能，以下分别进行详细说明。

为了更好的理解本申请提供的方案可以适用的领域以及场景，在本申请提供的技术方案进行具体的介绍之前，首先对人工智能主体框架、本申请提供的方案适用的系统架构以及神经网络的相关知识进行介绍。

图1示出一种人工智能主体框架示意图，该主体框架描述了人工智能系统总体工作流程，适用于通用的人工智能领域需求。

下面从“智能信息链”（水平轴）和“信息技术（information technology, IT）价值链”（垂直轴）两个维度对上述人工智能主题框架进行详细的阐述。

“智能信息链”反映从数据的获取到处理的一系列过程。举例来说，可以是智能信息感知、智能信息表示与形成、智能推理、智能决策、智能执行与输出的一般过程。在这个过程中，数据经历了“数据—信息—知识—智慧”的凝练过程。

“IT价值链”从人工智能的底层基础设施、信息（提供和处理技术实现）到系统的产业生态过程，反映人工智能为信息技术产业带来的价值。

（1）基础设施：

基础设施为人工智能系统提供计算能力支持，实现与外部世界的沟通，并通过基础平台实现支撑。

基础设施可以通过传感器与外部沟通，基础设施的计算能力可以由智能芯片提供。

这里的智能芯片可以是中央处理器（central processing unit, CPU）、神经网络处理器（neural-network processing unit, NPU）、图形处理器（graphics processing unit, GPU）、专门应用的集成电路（application specific integrated circuit, ASIC）以及现场可编程门阵列（field programmable gate array, FPGA）等硬件加速芯片。

基础设施的基础平台可以包括分布式计算框架及网络等相关的平台保障和支持，可以包括云存储和计算、互联互通网络等。

例如，对于基础设施来说，可以通过传感器和外部沟通获取数据，然后将这些数据提供给基础平台提供的分布式计算系统中的智能芯片进行计算。

（2）数据：

基础设施的上一层的数据用于表示人工智能领域的数据来源。该数据涉及到图形、图像、语音、文本，还涉及到传统设备的物联网数据，包括已有系统的业务数据以及力、位移、液位、温度、湿度等感知数据。

（3）数据处理：

上述数据处理通常包括数据训练，机器学习，深度学习，搜索，推理，决策等处理方式。

其中，机器学习和深度学习可以对数据进行符号化和形式化的智能信息建模、抽取、预处理、训练等。

5 推理是指在计算机或智能系统中，模拟人类的智能推理方式，依据推理控制策略，利用形式化的信息进行机器思维和求解问题的过程，典型的功能是搜索与匹配。

决策是指智能信息经过推理后进行决策的过程，通常提供分类、排序、预测等功能。

(4)通用能力：

10 对数据经过上面提到的数据处理后，进一步基于数据处理的结果可以形成一些通用的能力，比如可以是算法或者一个通用系统，例如，翻译，文本的分析，计算机视觉的处理，语音识别，图像的识别等等。

(5)智能产品及行业应用：

15 智能产品及行业应用指人工智能系统在各领域的产品和应用，是对人工智能整体解决方案的封装，将智能信息决策产品化、实现落地应用，其应用领域主要包括：智能制造、智能交通、智能家居、智能医疗、智能安防、自动驾驶，平安城市，智能终端等。

本申请实施例可以应用在人工智能中的很多领域，例如，智能制造、智能交通、智能家居、智能医疗、智能安防、自动驾驶，平安城市等领域。

具体地，本申请实施例可以具体应用在语音增强、语音识别需要使用(深度)神经网络的领域。

20 参见附图 2，本发明实施例提供了一种系统架构。数据采集设备 260 用于采集训练数据并存入数据库 230，其中，训练数据可以包括但不限于图像数据，音频数据，文本数据。以图像数据为例，训练数据可以包括不同域或者不同数据集的训练图像以及训练图像对应的标注结果（也称为标签）。其中，训练图像的标注结果可以是(人工)预先标注的训练图像中的各个待检测物体的分类结果。训练设备 220 基于数据库 230 中维护的训练数据生成
25 目标模型/规则 201。

上述目标模型/规则 201 能够用于实现本申请实施例的数据处理的方法，即，将待处理数据(或者通过相关预处理后)输入该目标模型/规则 201，即可得到待处理数据的检测结果或者针对待处理数据的预测结果。本申请实施例中的目标模型/规则 201 具体可以为神经网络。

30 还包括计算模块 211，计算模块中包括目标模型/规则 201，根据训练设备 220 训练得到的目标模型/规则 201 可以应用于不同的系统或设备中，如应用于图 2 所示的执行设备 210，所述执行设备 210 可以是终端，如手机终端，平板电脑，笔记本电脑，增强现实(augmented reality, AR)/虚拟现实(virtual reality, VR)，车载终端，用于安防的设备（比如监控摄像设备、烟雾报警设备、灭火设备），智能音箱，物联网(the internet of
35 things)设备等。还可以是服务器或者云端等。在图 2 中，执行设备 210 配置输入/输出(input/output, I/O)接口 212，用于与外部设备进行数据交互，用户可以通过客户设备 240 向 I/O 接口 212 输入数据，所述输入数据在本申请实施例中可以包括：客户设备输入的待

处理图像数据，待处理文本数据，待处理语音数据等等。这里的客户设备 240 具体可以是终端设备。

在图 2 中所示情况下，用户可以手动给定输入数据，该手动给定可以通过 I/O 接口 212 提供的界面进行操作。另一种情况下，客户设备 240 可以自动地向 I/O 接口 212 发送输入数据，如果要求客户设备 240 自动发送输入数据需要获得用户的授权，则用户可以在客户设备 240 中设置相应权限。用户可以在客户设备 240 查看执行设备 210 输出的结果，具体的呈现形式可以是显示、声音、动作等具体方式。客户设备 240 也可以作为数据采集端，采集如图所示输入 I/O 接口 212 的输入数据及输出 I/O 接口 212 的输出结果作为新的样本数据，并存入数据库 230。当然，也可以不经过客户设备 240 进行采集，而是由 I/O 接口 212 直接将如图所示输入 I/O 接口 112 的输入数据及输出 I/O 接口 112 的输出结果，作为新的样本数据存入数据库 230。

下面对训练设备 220 如何基于训练数据得到目标模型/规则 201 进行描述，目标模型/规则 201 能够执行不同的任务，比如目标模型/规则 201 可以用于执行分类任务，回归任务，等等，可以将任务理解为从数据中自动分析获得规律，并利用规律对未知数据进行预测的算法。

神经网络中的每一层的工作可以用数学表达式 $\vec{y} = \alpha(W\vec{x} + b)$ 来描述：从物理层面神经网络中的每一层的工作可以理解为由通过五种对输入空间（输入向量的集合）的操作，完成输入空间到输出空间的变换（即矩阵的行空间到列空间），这五种操作包括：1、升维/降维；2、放大/缩小；3、旋转；4、平移；5、“弯曲”。其中 1、2、3 的操作由 $W\vec{x}$ 完成，4 的操作由 $+b$ 完成，5 的操作则由 $\alpha()$ 来实现。这里之所以用“空间”二字来表述是因为被分类的对象并不是单个事物，而是一类事物，空间是指这类事物所有个体的集合。其中， W 是权重向量，该向量中的每一个值表示该层神经网络中的一个神经元的权重值。该向量 W 决定着上文所述的输入空间到输出空间的空间变换，即每一层的权重 W 控制着如何变换空间。训练神经网络的目的，也就是最终得到训练好的神经网络的所有层的权重矩阵（由很多层的向量 W 形成的权重矩阵）。因此，神经网络的训练过程本质上就是学习控制空间变换的方式，更具体的就是学习权重矩阵。

因为希望深度神经网络的输出尽可能的接近真正想要预测的值，所以可以通过比较当前网络的预测值和真正想要的目标值，再根据两者之间的差异情况来更新每一层神经网络的权重向量（当然，在第一次更新之前通常会有初始化的过程，即为神经网络中的各层预先配置参数），比如，如果网络的预测值高了，就调整权重向量让它预测低一些，不断的调整，直到神经网络能够预测出真正想要的目标值。因此，就需要预先定义“如何比较预测值和目标值之间的差异”，这便是损失函数(loss function)或目标函数(objective function)，它们是用于衡量预测值和目标值的差异的重要方程。其中，以损失函数举例，损失函数的输出值(loss)越高表示差异越大，那么深度神经网络的训练就变成了尽可能缩小这个 loss 的过程。

训练设备 220 得到的目标模型/规则可以应用不同的系统或设备中。在附图 2 中，执行设备 210 配置有 I/O 接口 212，与外部设备进行数据交互，“用户”可以通过客户设备 240

向 I/O 接口 212 输入数据。

执行设备 210 可以调用数据存储系统 250 中的数据、代码等，也可以将数据、指令等存入数据存储系统 250 中。

5 卷积神经网络 (convolutional neuron nrtwork, CNN) 是一种带有卷积结构的深度神经网络，是一种深度学习 (deep learning) 架构，深度学习架构是指通过机器学习的算法，在不同的抽象层级上进行多个层次的学习。作为一种深度学习架构，CNN 是一种前馈 (feed-forward) 人工神经网络，该前馈人工神经网络中的各个神经元对输入其中的图像中的重叠区域作出响应。

10 如图 3 所示，卷积神经网络 (CNN) 100 可以包括输入层 110，卷积层/池化层 120，其中池化层为可选的，以及神经网络层 130。

卷积层/池化层 120：

卷积层：

15 如图 3 所示卷积层/池化层 120 可以包括如示例 121-126 层，在一种实现中，121 层为卷积层，122 层为池化层，123 层为卷积层，124 层为池化层，125 为卷积层，126 为池化层；在另一种实现方式中，121、122 为卷积层，123 为池化层，124、125 为卷积层，126 为池化层。即卷积层的输出可以作为随后的池化层的输入，也可以作为另一个卷积层的输入以继续进行卷积操作。

20 以卷积层 121 为例，卷积层 121 可以包括很多个卷积算子，卷积算子也称为核，其在图像处理中的作用相当于一个从输入图像矩阵中提取特定信息的过滤器，卷积算子本质上可以是一个权重矩阵，这个权重矩阵通常被预先定义，在对图像进行卷积操作的过程中，权重矩阵通常在输入图像上沿着水平方向一个像素接着一个像素（或两个像素接着两个像素……这取决于步长 stride 的取值）的进行处理，从而完成从图像中提取特定特征的工作。该权重矩阵的大小应该与图像的大小相关，需要注意的是，权重矩阵的纵深维度 (depth dimension) 和输入图像的纵深维度是相同的，在进行卷积运算的过程中，权重矩阵会延伸到输入图像的整个深度。因此，和一个单一的权重矩阵进行卷积会产生一个单一纵深维度的卷积化输出，但是大多数情况下不使用单一权重矩阵，而是应用维度相同的多个权重矩阵。每个权重矩阵的输出被堆叠起来形成卷积图像的纵深维度。不同的权重矩阵可以用来提取图像中不同的特征，例如一个权重矩阵用来提取图像边缘信息，另一个权重矩阵用来提取图像的特定颜色，又一个权重矩阵用来对图像中不需要的噪点进行模糊化……该多个权重矩阵维度相同，经过该多个维度相同的权重矩阵提取后的特征图维度也相同，再将提取到的多个维度相同的特征图合并形成卷积运算的输出。

25 这些权重矩阵中的权重值在实际应用中需要经过大量的训练得到，通过训练得到的权重值形成的各个权重矩阵可以从输入图像中提取信息，从而帮助卷积神经网络 100 进行正确的预测。

35 当卷积神经网络 100 有多个卷积层的时候，初始的卷积层（例如 121）往往提取较多的一般特征，该一般特征也可以称之为低级别的特征；随着卷积神经网络 100 深度的加深，越往后的卷积层（例如 126）提取到的特征越来越复杂，比如高级别的语义之类的特征，

语义越高的特征越适用于待解决的问题。

池化层：

由于常常需要减少训练参数的数量，因此卷积层之后常常需要周期性的引入池化层，即如图 3 中 120 所示例的 121-126 各层，可以是一层卷积层后面跟一层池化层，也可以是 5 多层卷积层后面接一层或多层池化层。以图像数据为例，在图像处理过程中，池化层的唯一目的就是减少图像的空间大小。池化层可以包括平均池化算子和/或最大池化算子，以用于对输入图像进行采样得到较小尺寸的图像。平均池化算子可以在特定范围内对图像中的像素值进行计算产生平均值。最大池化算子可以在特定范围内取该范围内值最大的像素作为最大池化的结果。另外，就像卷积层中用权重矩阵的大小应该与图像大小相关一样，池化层中的运算符也应该与图像的大小相关。通过池化层处理后输出的图像尺寸可以小于输入池化层的图像的尺寸，池化层输出的图像中每个像素点表示输入池化层的图像的对子区域的平均值或最大值。

神经网络层 130：

在经过卷积层/池化层 120 的处理后，卷积神经网络 100 还不足以输出所需要的输出信息。因为如前所述，卷积层/池化层 120 只会提取特征，并减少输入图像带来的参数。然而 15 为了生成最终的输出信息（所需要的类信息或别的相关信息），卷积神经网络 100 需要利用神经网络层 130 来生成一个或者一组所需要的类的数量的输出。因此，在神经网络层 130 中可以包括多层隐含层（如图 3 所示的 131、132 至 13n）以及输出层 140，该多层隐含层中所包含的参数可以根据具体的任务类型的相关训练数据进行预先训练得到，例如该任务 20 类型可以包括图像识别，图像分类，图像超分辨率重建等等……。

在神经网络层 130 中的多层隐含层之后，也就是整个卷积神经网络 100 的最后层为输出层 140，该输出层 140 具有类似分类交叉熵的损失函数，具体用于计算预测误差，一旦整个卷积神经网络 100 的前向传播（如图 3 由 110 至 140 的传播为前向传播）完成，反向传播（如图 3 由 140 至 110 的传播为反向传播）就会开始更新前面提到的各层的权重值以及偏差，以减少卷积神经网络 100 的损失及卷积神经网络 100 通过输出层输出的结果和理想结果之间的误差。

需要说明的是，如图 3 所示的卷积神经网络 100 仅作为一种卷积神经网络的示例，在具体的应用中，卷积神经网络还可以以其他网络模型的形式存在，例如，如图 4 所示的多个卷积层/池化层并行，将分别提取的特征均输入给神经网络层 130 进行处理。

30 本申请提供的方案适应于一种机器学习系统，该机器学习系统包括服务器和至少一个端侧设备，本申请以该机器学习系统是联邦学习系统为例进行说明，为了更好的理解本申请提供的方案，下面对联邦学习的相关知识进行介绍。

参阅图 5，为一种联邦学习系统的架构示意图。联邦学习是一种用于用户隐私保护的机器学习技术，联邦学习系统结构上一般包括一个中心服务器和多个客户端作为参与方， 35 工作流程主要包括模型下发和模型融合过程。在模型下发过程，客户端从中心服务器下载模型，通过本地存储的训练数据对从中心服务器上下载模型进行训练，训练到一定程度后上传模型到中心服务器，其中训练到一定程度可以理解为训练固定轮数。在模型融合过

程中，中心服务器会收集各个客户端上传的模型，并进行模型融合。模型下发过程和模型融合过程这两个过程会反复迭代直至模型收敛。需要说明的是，本申请有时也将中心服务器称为服务器，二者表示相同的意思，在一些可能的实施方式中，该服务器可以是云服务器或者云侧设备，本申请实施例对此并不进行限定。本申请有时也将客户端称为端侧设备，

5 二者表示相同的意思，比如端侧设备可以是终端，如手机终端，平板电脑，笔记本电脑，增强现实(augmented reality, AR)/虚拟现实(virtual reality, VR)，车载终端，用于安防的设备（比如监控摄像设备、烟雾报警设备、灭火设备），智能音箱等。此外，需要说明的是，本申请中的模型包括神经网络模型，本申请对模型的具体类别并不进行限定，比如本申请中的模型可以是卷积神经网络模型，循环神经网络模型，深度残差网络模型等等。

10 参阅图 6，在图 5 所示的联邦学习系统的基础上，一种适用于联邦学习系统的模型训练方法的流程示意图。在联邦学习系统中，多个客户端中各个客户端执行的流程相似，在图 6 所示的流程中，以多个客户端中的其中一个客户端为例，说明联邦学习系统中的模型训练方法。在对模型训练之前，包括一个初始化的阶段，在初始化的阶段，包括步骤 601、服务器向多个客户端中的各个客户端发送初始的模型，各个客户端接收到初始的模型后，

15 包括步骤 602、利用本地的训练数据对接收到的初始的模型进行训练，训练到一定程度后，执行步骤 603、将训练到一定程度的初始的模型发送至服务器。其中，对初始的模型训练到一定程度可以理解是对初始的模型训练 N 轮，其中 N 为预先的正整数，本申请中以下关于将某个模型训练到一定程度都可以理解为将某个模型训练预设的轮数，本申请对此不再进行重复说明。此外，对模型训练一轮可以理解为对训练数据遍历一轮后，模型输出一次

20 预测结果，并根据预测结果和第一标签对模型的权重参数进行一次更新的过程。服务器接收到各个客户端发送的训练到一定程度的初始的模型后，执行步骤 604、对接收到的训练到一定程度的初始的模型进行融合处理，以得到共享模型 1。对多个模型进行融合处理的方式可以有多种，比如服务器可以对接收到的多个模型进行求平均值处理，将多个模型进行求平均值后的结果作为共享模型，再比如服务器对接收到的多个模型进行加权处理，将

25 多个模型进行加权处理后的结果作为共享模型。如下公式 1-1 给出了一种服务器对接收到的多个模型进行融合，得到共享模型的方式。

$$M = \sum_{K=1}^K \frac{N_K}{N} M_K \quad (1-1)$$

上述公式 1-1 中，M 代表共享模型，K 代表一共有 K 个客户端， N_K 代表第 K 个客户端上训练样本的数据量，N 代表所有客户端上训练样本的总数据量， M_K 代表第 K 个客户端发

30 送的训练到一定程度的模型。上述公式 1-1 用于表示服务器对接收到的 K 个客户端发送的模型 M_K 进行融合处理得到共享模型 M，并且一个客户端上的训练样本的数据量越大，则在

进行加权融合处理时，对该客户端训练得到的模型分配越高的权重。

服务器得到共享模型 1 后，执行步骤 605、将共享模型 1 向各个客户端发送。客户端接收到共享模型 1 后，执行步骤 606、通过共享模型 1 更新本地存储的训练到一定程度的

35 初始的模型，并对共享模型 1 进行训练，得到训练到一定程度的共享模型 1。执行步骤 607、

客户端将训练到一定程度的共享模型 1 向服务器发送,以使服务器执行步骤 608、对各个客户端发送的训练到一定程度的共享模型 1 进行融合处理,以得到新的共享模型,这里称为共享模型 2,共享模型 2 用于更新共享模型 1。其中,客户端将训练到一定程度的共享模型 1 向服务器发送,可以理解为客户端发送的是完整的训练到一定程度的共享模型 1,也可以理解为客户端发送的是训练到一定程度的共享模型 1 的全部权重参数,或者可以理解客户端发送的是训练到一定程度的共享模型 1 的部分权重参数,这里的部分权重参数是训练到一定程度的共享模型 1 相比于训练到一定程度的初始的模型有更新的权重参数。下面以一个简单的例子对客户端将训练到一定程度的共享模型 1 向服务器发送进行示意性的说明,其中一种方式为将完整的训练到一定程度的共享模型 1 发送至服务器,假设完整的训练到一定程度的共享模型 1 一共包括权重参数 A,权重参数 B 以及权重参数 C,则客户端发送的是训练到一定程度的共享模型 1 的全部权重参数可以理解为客户端只向服务器发送权重参数 A,参数权重 B 以及权重参数 C。再比如由于训练到一定程度的初始的模型也包括权重参数 A,权重参数 B 以及权重参数 C,假设确定训练到一定程度的共享模型 1 相比于训练到一定程度的初始的模型,权重参数 A 发生了变换(权重参数的取值有更新),权重参数 B 和权重参数 C 没有发生变换,则客户端发送的是训练到第一程度的共享模型 1 的部分权重参数可以理解为客户端只向服务器发送权重参数 A。

下面公式 1-2 给了一种服务器对接收到的训练到一定程度的共享模型 1 进行融合处理,以得到共享模型 2 的方式。

$$M' = M + \sum_{k=1}^K \frac{N_k}{N} \Delta k \quad (1-2)$$

其中, M' 表示共享模型 2, Δk 表示训练到一定程度的共享模型 1 相比于训练到一定程度的初始的模型有更新的权重参数。 M 、 K 、 N 以及 N_k 参照公式 1-1 进行理解,这里不再重复解释。

服务器可以执行步骤 609、将共享模型 2 再次向各个客户端进行发送,以使客户端对接收到的模型进行训练,并将训练到一定程度的模型再次向服务器发送,这是一个循环执行的过程,即服务器对接收到的各个客户端发送的模型进行融合处理,并将经过融合处理得到的模型发送至各个客户端,客户端对接收到的服务器发送的模型进行训练,并将训练到第一程度的模型发送到服务器。在一个可能的实施方式中,客户端可以认为当前接收到的模型为收敛的模型,即认为当前接收到的模型为最终的模型,则客户端不再对当前接收到的模型进行训练,也不再接受服务器发送的共享模型,客户端可以利用当前接收到的模型执行推理任务。比如客户端可以预先设定接收到的第 N 个模型为最终的模型,接收到 N 个模型后,则认为模型训练结束,不再接受服务器发送的共享模型。在一个可能的实施方式中,客户端可以认为当前训练得到的模型为收敛的模型,即认为当前训练得到的模型为最终的模型,则客户端不再将当前训练到一定程度的模型向服务器发送,也不再接受服务器后续发送的共享模型,客户端可以利用当前训练到一定程度的模型执行推理任务。比如客户端可以预先设定对接收到的第 N 个模型训练到一定程度的模型为最终的模型,则客户端接收到第 N 个模型,并对该模型训练到一定程度后,可以认为训练结束。以上两种实施

方式为从客户端的角度确定停止训练的方式，在一些可能的实施方式中，也可以由服务器确定停止训练，比如服务器认为第 N 次下发的模型为最终的模型，则服务器下发了第 N 次模型后，可以向各个客户端发送通知指令，该通知指令用于通知各个客户端训练完成。

在图 6 所示的联邦学习系统的一种训练模型的方式中，存在单个共享模型难以适配所有客户端的数据分布的问题，这是因为参与联邦学习训练的客户端上的数据分布往往是非独立同分布 (non-independent and identically, Non-IID) 的，数据分布之间存在较大差异，难以使用一个单独的模型拟合所有数据分布。其中，数据分布不同可以理解为同一个标签在不同客户端的训练数据集中的比例不同。

综合以上的考虑，本申请提供了一种训练模型的方法，解决单一模型难以适配所有客户端上非独立同分布的数据的问题，且通过本申请提供的训练模型的方法，避免私有模型产生过拟合的问题。本申请提供的方案适用于联邦学习系统，通过本申请提供的方案，使端侧设备训练得到的模型性能更优。下面对本申请提供的方案进行具体的介绍。

参阅图 7，为本申请实施例提供的一种联邦学习系统的架构示意图。如图 7 所示，本申请提供的一种联邦学习系统包括服务器和至少两个端侧设备。其中，服务器可以是实体设备，或者将服务器的物理资源抽象成逻辑资源，让一台服务器成为多台独立的虚拟服务器，或者让几台服务器作为一台服务器来使用。在一个可能的实现方式中，服务器为云端的虚拟机 (virtual machine, VM)。各个端侧设备和服务器的交互流程是相同的，以下在介绍本申请提供的一种训练模型的方法时，以第一端侧设备为例对端侧设备和服务器之间的交互流程，以及端侧设备的训练过程进行说明。其中，第一端侧设备可以理解为至少两个端侧设备中的任意一个端侧设备。

继续参阅图 7，针对第一端侧设备，第一端侧设备中存储有两个模型，其中一个模型直接参与联邦学习的过程，另一个模型不直接参与联邦学习的过程。以下将直接参与联邦学习的过程的模型称为共享模型，将不直接参与联邦学习和融合过程的模型称为私有模型。本申请提供的方案根据本地存储的训练数据以及共享模型在联邦学习过程中学习到的知识更新私有模型。以下对训练过程进行具体的介绍。

参阅图 8，为本申请实施例提供的一种训练模型的方法的流程示意图。本申请提供的一种训练模型的方法，可以包括以下步骤：

900、服务器向第一端侧设备发送初始的共享模型。

图 7 描述联邦学习系统的架构时介绍到端侧设备存储有两个模型，一个是共享模型，一个是私有模型。第一端侧设备向服务器发送共享模型，不向服务器发送私有模型，其中共享模型参与联邦学习和融合的过程。参与联邦学习和融合的过程可以参照步骤 902 至步骤 904、以及 909 至 910 进行理解，将在后文进行详细介绍。私有模型是第一端侧设备本地存储的一个模型。

在初始状态下，其中初始状态可以理解为还没有开始训练过程之前，端侧设备上存储有初始的私有模型和初始的共享模型。本文关于模型的理解均参照上文中关于模型的定义进行理解，本申请中的模型包括神经网络模型，本申请对模型的具体类别并不进行限定，比如本申请中的模型可以是卷积神经网络模型，循环神经网络模型，深度残差网络模型等

等。以下对于模型的定义和理解不再重复说明。

初始的共享模型是第一端侧设备从服务器中获取的模型，即在初始状态下，服务器向第一端侧设备发送初始的共享模型，各个端侧设备接收到的初始的共享模型是相同的。第一端侧设备接收服务器发送的初始的共享模型并保存，以便对该初始的共享模型进行训练。

5 初始的私有模型是第一端侧设备本地存储的一个模型，该初始的私有模型和初始的共享模型可以是不同类型的模型，比如可以是异构的神经网络，初始的私有模型和初始的共享模型可以用于不同的任务，比如初始的共享模型采用多层感知器 (multilayer perceptron, MLP) 对图像进行分类，初始的私有模型采用反卷积神经网络对图像进行重构。初始的私有模型和初始的共享模型也可以用于执行相同的任务。

10 901、第一端侧设备向服务器发送第一共享模型。

其中，第一共享模型可以理解为第一端侧设备对初始的共享模型进行训练后，得到的模型，比如第一共享模型是第一端侧设备通过本地存储的训练数据对初始的共享模型训练到一定程度后得到的模型。

此外，需要说明的是，第一端侧设备向服务器发送第一共享模型可以理解为第一端侧设备向服务器发送第一共享模型的全部权重参数。或者第一端侧设备向服务器发送第一共享模型可以理解为第一端侧设备向服务器发送第一共享模型的部分权重参数，比如，如果第一共享模型是第一端侧设备对初始的共享模型训练到一定程度获取的，其中部分权重参数是指第一共享模型和初始的共享模型不同的权重参数。

15 在一个优选的实施方式中，参阅图 8-a 进行理解，共享模型和私有模型可以采用共享的特征提取模型。共享模型和私有模型采用的特征提取模型，有利于后续的融合处理过程。在图 8 对应的实施例中，即服务器发送的初始的共享模型包括初始的特征提取模型和初始的任务模型，第一端侧设备接收到服务器发送的初始的共享模型后，将初始的私有模型中的特征提取模型更新为从服务器接收到的初始的特征提取模型。或者初始的私有模型直接采用从服务器接收到的初始的特征提取模型。其中任务模型可以理解为用于执行不同任务的模型，比如用于执行分类任务的模型，用于执行回归任务的模型等等。可以将任务理解为从数据中自动分析获得规律，并利用规律对未知数据进行预测的算法。

20 902、服务器根据至少两个端侧设备发送的第一共享模型进行融合处理，以获取第二共享模型。

服务器可以采用多种融合算法对接收到的多个第一共享模型进行融合处理，以获取第二共享模型。比如可以对多个第一共享模型求平均值以获取第二共享模型，或者可以对多个第一共享模型进行加权处理，以获取第二共享模型，或者可以采用其他预设的算法对多个第一共享模型进行处理，以获取第二共享模型。

30 在一个可能的实施方式中，第一共享模型包括特征提取模型和任务模型，比如第一共享模型包括特征提取模型 1 和任务模型 1。继续参阅图 8-a，服务器对各个端侧设备发送的特征提取模型 1 进行融合处理，得到特征提取模型 2，服务器对各个端侧设备发送的任务模型 1 进行融合处理，得到任务模型 2，第二共享模型包括特征提取模型 2 和任务模型 2。如下公式 2-1 给出一种服务器对各个端侧设备发送的特征提取模型进行融合处理的方式，

公式 2-2 给出了一种服务器对各个端侧设备发送的任务模型进行融合处理的方式。

$$F = \frac{1}{N} \sum_{K=1}^K N_K F_K \quad (2-1)$$

$$C_s = \frac{1}{N} \sum_{K=1}^K N_K C_{s,K} \quad (2-2)$$

其中，F 代表融合后的特征提取模型，Cs 代表融合后的任务模型， N_K 代表第 K 个客户端上训练样本的数据量，N 代表所有客户端上训练样本的总数据量， F_K 代表第 K 个客户端发送的第一共享模型中的特征提取模型，比如特征提取模型 1， $C_{s,K}$ 代表第 K 个客户端发送的第一共享模型的任务模型，比如任务模型 1。

903、第一端侧设备接收服务器发送的第二共享模型。

服务器根据至少两个端侧设备发送的第一共享模型进行融合处理，以获取第二共享模型后，向各个端侧设备发送第二共享模型。

在一个可能的实施方式中，如果共享模型和私有模型采用相同的特征提取模型，则第一端侧设备接收到服务器发送的第二共享模型后，通过第二共享模型的特征提取模型更新本地存储的私有模型的特征提取模型。

904、通过第二共享模型输出针对训练数据集的第一预测结果。

可以将训练数据集输入到第二共享模型中，以输出训练数据集的第一预测结果。

以第二共享模型用于执行分类任务为例进行说明，第一端侧设备可以获取样本数据集，样本数据集包括多个样本，多个样本中的每个样本均包括第一标签。可以用第二共享模型对训练数据集进行分类，得到测试数据集中的每个样本的第二标签，可以将第一预测结果理解为第二标签。

905、第一端侧设备根据第一预测结果获取第一损失值。

第一损失值用于表示第一标签和第二标签的差异。

906、第一端侧设备通过第一私有模型输出针对训练数据集的第二预测结果。

可以将训练数据集输入到第一私有模型中，以输出训练数据集的第一预测结果。

以第一私有模型用于执行分类任务为例进行说明，第一端侧设备可以获取样本数据集，样本数据集包括多个样本，多个样本中的每个样本均包括第一标签。可以用第一私有模型对训练数据集进行分类，得到测试数据集中的每个样本的第三标签，可以将第二预测结果理解为第三标签。

在一个可能的实施方式中，如果共享模型和私有模型采用相同的特征提取模型，则第一端侧设备接收到服务器发送的第二共享模型后，通过第二共享模型的特征提取模型更新本地存储的私有模型的特征提取模型。步骤 906 中的第一模型是指更新了特征提取模型的私有模型，即步骤 906 中描述的第一私有模型和步骤 904 中描述的第二共享模型的特征提取模型是相同的。

907、第一端侧设备根据第二预测结果获取第二损失值。

第二损失值用于表示第一标签和第三标签的差异。

需要说明的是步骤 904 和步骤 906 在执行上不区分先后顺序，比如可以同时获取第一预测结果和第二预测结果。

908、第一端侧设备对第一损失值和第二损失值进行第二融合处理，以获取第三损失值，第三损失值用于更新私有模型。

第一损失值和第二损失值可以是不同类别的损失值，比如第一损失值包括交叉熵损失值，双向蒸馏损失值，正则化范数损失值中的一个或者多个，第二损失值包括交叉熵损失值，双向蒸馏损失值，正则化范数损失值中的一个或者多个。示例性的，下面给出几种对第一损失值和第二损失值进行融合处理，以获取第三损失值的方式。

在一个可能的实施方式中，第一损失值是交叉熵损失值，第二损失值是交叉熵损失值。第一损失值的计算公式如公式 2-3 所示，第二损失值的计算公式如公式 2-4 所示，第三损失值的计算公式如公式 2-5 所示。

$$\begin{aligned} L_{11} &= -\sum_i y_{s,i,c} \log\left(\frac{\exp(g_{s,i,c})}{\sum_{c'} \exp(g_{s,i,c'})}\right) \quad (2-3) \\ L_{21} &= -\sum_i y_{p,i,c} \log\left(\frac{\exp(g_{p,i,c})}{\sum_{c'} \exp(g_{p,i,c'})}\right) \quad (2-3) \\ L1 &= \gamma_1 L_{11} + \gamma_2 L_{21} \quad (2-4) \end{aligned}$$

其中，L11 代表第一损失值，i 代表第 i 个样本， y_i 表示第 i 个样本的第一标签， $y_{s,i,c}$ 表示第 i 个样本被共享模型分为 C 类的概率， $y_{p,i,c}$ 表示第 i 个样本被私有模型分为 C 类的概率。在一个可能的实施方式中，当第 i 个样本在 C 类的 $y_{p,i,c}$ 值最大时，则第 i 个样本被私有模型分为 C 类；当第 i 个样本在 C 类的 $y_{s,i,c}$ 最大时，则第 i 个样本被共享模型分为 C 类。 $g_{s,i,c}$ 表示第 i 个样本在共享模型上被分为 C 类的概率， $\sum_{c'} \exp(g_{s,i,c'})$ 表示对于共享模型，预测结果中所有种类的概率值的指数函数求和。 L_{21} 代表第二损失值， $(g_{p,i,c})$ 代表第 i 个样本在私有模型上被分为 C 类的概率， $\sum_{c'} \exp(g_{p,i,c'})$ 表示对于私有模型，预测结果中所有种类的概率值的指数函数求和。L1 代表第三损失值， γ_1 和 γ_2 为预先设定的系数，其中 γ_1 和 γ_2 均为 0 至 1 范围内的实数，并且 γ_1 和 γ_2 的和为 1。

在一个可能的实施方式中，第一损失函数是双向知识蒸馏损失，第二损失函数是双向知识蒸馏损失。第一损失值的计算公式如公式 2-5 所示，第二损失值的计算公式如公式 2-6 所示，第三损失值的计算公式如公式 2-7 所示。

$$\begin{aligned} L_{12}(T) &= KL(\text{softmax}(g_s, T), \text{softmax}(g_p, 1)) \quad (2-5) \\ L_{22}(T) &= KL(\text{softmax}(g_p, T), \text{softmax}(g_s, 1)) \quad (2-6) \\ L2 &= \mu_1 L_{12} + \mu_2 L_{22} \quad (2-7) \end{aligned}$$

其中，L12 代表第一损失值，L22 代表第二损失值，L2 代表第三损失函数， μ_1 和 μ_2 为预先设定的系数，T 是预先设定的温度系数，其中 T 是不小于 1 的实数，在一个可能的实施方式中，为了便于计算 T 可以是正整数，比如 T 可以是不小于 1 且不大于 50 的正整数。 g_s 代表第一端侧设备上的训练数据集在不同类别的预测概率的向量， g_p 代表第一端侧设备

上的训练数据集在不同类别的预测概率的向量。KL()是一种用来衡量向量分布的差异的函数。可以参照公式 2-8 进行理解。

$$KL(p, q) = \sum_c p_c \log \frac{p_c}{q_c} \quad (2-8)$$

其中, p_c 代表 p 向量的第 c 个维度, q_c 代表 q 向量的第 c 个维度。

5 softmax() 是一种归一化指数函数, 可以参照公式 2-9 进行理解。

$$\text{softmax}(g, T) = \frac{\exp(g_c/T)}{\sum_{c'} \exp(g_{c'}/T)}, \text{ 对于 } g \text{ 中任一维度 } c \quad (2-9)$$

其中, g 是一个向量, g 可能包括多个维度, 公式 2-9 表示针对多个维度中的一个维度 g_c 求解 softmax(g, T), g_c 是向量 g 的第 c 个维度, $g_{c'}$ 是向量 g 的所有维度。

10 在一个可能的实施方式中, 第一损失值是交叉熵损失值, 第二损失值是双向知识蒸馏损失, 则第三损失值还可以参照公式 2-10 进行理解。

$$L3 = \varepsilon_1 L_{11} + \varepsilon_2 L_{22} \quad (2-10)$$

其中, L3 表示另一种第三损失值的计算方式。

在一个可能的实施方式中, 第一损失值包括交叉熵损失值和双向知识蒸馏损失, 第二损失值是双向指示蒸馏损失, 则第三损失值还可以参照公式 2-11 进行理解。

$$15 \quad L4 = \delta_1 L_{11} + \delta_2 L_{12} + \delta_3 L_{22} \quad (2-11)$$

其中, L4 表示另一种第三损失值的计算方式。 δ_1 、 δ_2 以及 δ_3 均为实数, 且 δ_1 、 δ_2 以及 δ_3 的和为 1。

20 在一个可能的实施方式中, 第一损失值包括交叉熵损失值和双向知识蒸馏损失, 第二损失值包括交叉熵损失值和双向指示蒸馏损失, 则第三损失值还可以参照公式 2-11 进行理解。

$$L5 = \varphi_1 L_{11} + \varphi_2 L_{12} + \varphi_3 L_{21} + \varphi_4 L_{22} \quad (2-11)$$

其中, L5 表示另一种第三损失值的计算方式。

在一个可能的实施方式中, 第三损失值还可以参照公式 2-12 进行理解。

$$L6 = \sum_i w_i (\theta_{p,i} - \theta_{s,i})^2 \quad (2-12)$$

25 其中, L6 表示另一种第三损失值的计算方式, w_i 代表权重值, 针对不同的样本设定不同的权重, $\theta_{p,i}$ 表示端侧上训练到一定程度的私有模型的第 i 个权重参数, $\theta_{s,i}$ 表示端侧设备上训练到一定程度的共享模型的第 i 个权重参数。

需要说明的是, 可以通过对第一损失值和第二损失值进行加权处理, 以获取第三损失值, 或者可以通过对第一损失值和第二损失值求平均值, 以获取第三损失值。上面列举的
30 几种对第一损失值和第二损失值进行融合处理, 以获取第三损失值的方案并不代表穷举, 除了上述列举的几种根据第一损失值和第二损失值确定第三损失值的方案, 本申请还可以包括其他根据第一损失值和第二损失值确定第三损失值的方案, 比如第三损失值还可以是 L5 和 L6 的加和等等。此外, 第一损失值包括但不限于交叉熵损失值, 双向蒸馏损失值, 正则化范数损失值, 第二损失值包括但不限于交叉熵损失值, 双向蒸馏损失值, 正则化范

数损失值。

可以采用多种方式实现通过第三损失值更新私有模型，比如可以采用梯度优化方法，通过第三损失值更新私有模型，具体的可以更新私有模型的特征提取模型的权重参数以及私有模型的任务模型的权重参数。

- 5 通过第三损失值更新私有模型后，还可以对更新的私有模型继续训练，比如继续对更新的私有模型训练固定的轮数，已得到更新后的私有模型。

在一个可能的实施方式中，还可以步骤 909、向服务器发送第三共享模型。

- 10 第三损失值除了用于更新私有模型之外，还可以用于更新第二共享模型，以得到第三共享模型。具体的，第三损失值用于更新第二共享模型的特征提取模型和任务模型，比如更新后的第二共享模型的特征提取模型是特征提取模型 2，更新后的第二共享模型的任务模型是任务模型 2，则第三共享模型包括特征提取模型 2 和任务模型 2。

通过第三损失值更新第二共享模型后，还可以对更新的第二共享模型继续训练，训练到固定轮数后得到第三共享模型，其中固定轮数可以预先设定。

对应于步骤 909，还可以包括步骤 910、服务器根据第三共享模型更新第二共享模型。

- 15 服务器接收到各个端侧设备发送的第三共享模型后，对各个端侧设备发送的第三共享模型进行融合处理，以得到第四共享模型，通过第四共享模型更新第二共享模型。

- 上述步骤 901 至步骤 910 可以是一个循环执行的过程，即服务器对接收到的各个端侧设备发送的共享模型进行融合处理，并将融合处理后的共享模型发送至各个端侧设备，端侧设备对接收到的共享模型进行训练，并利用该共享模型更新本地存储的私有模型，端侧设备还将训练到一定程度后的共享模型发送至服务器，这一过程会一直重复执行直至满足停止训练的条件。在一个可能的实施方式中，可以由端侧设备确定停止训练，比如端侧设备可以预先设定对接收到的第 N 个模型训练到一定程度的模型为最终的模型，则端侧设备接收到第 N 个模型，并对该模型训练到一定程度后，可以认为训练结束。训练接收后，端侧设备不再将训练到一定程度后的模型向服务器发送，端侧设备也不再从服务器侧接收模型，端侧设备可以利用最终得到的模型去执行推理任务，比如去执行分类任务，回归任务等等。再比如端侧设备可以预先设定接收到的第 N 个模型为最终的模型，接收到 N 个模型后，则认为模型训练结束。在一个可能的实施方式中，可以由服务器确定停止训练，比如服务器认为第 N 次下发的模型为最终的模型，则服务器下发了第 N 次模型后，可以向各个客户端发送通知指令，该通知指令用于通知各个客户端训练完成。

- 30 由图 8 对应的实施例可知，本申请提供的方案在端侧设备上训练两个模型，一个模型参与联邦学习和融合的过程，一个模型不直接参与联邦学习和融合的过程，根据训练后的两个模型分别获取两个模型的损失值，对两个模型的损失值进行融合，并通过融合后的损失值更新该两个模型，实现两个模型之间的信息传递，以使端侧设备训练得到的私有模型性能更优。此外通过本申请提供的方案，也可以解决由于端侧设备的训练数据集的训练样本的数据较少时，可能会出现私有模型过拟合的问题。

在一些可能的应用场景中，端侧设备可能对数据的隐私保护有很高的需求，则可以对端侧设备的训练数据按照需要隐私保护的高低进行划分，其中对隐私保护要求高的数据仅

参与私有模型的训练过程，其余的数据可以既参与共享模型的训练过程也参与私有模型的训练过程，下面对此进行详细的说明。

在上述图 8 对应的实施例的基础上继续进行说明，在一个可能的实施方式中，训练数据集包括第一训练数据集和第二训练数据集，第一训练数据集预先设定需要隐私保护，第二训练数据集预先设定不需要隐私保护，第一训练数据集和第二训练数据集用于对端侧设备存储的私有模型进行训练，以得到训练后的私有模型，第二训练数据集还用于对第二共享模型进行训练，以得到训练后的第二共享模型。参阅图 9，为本申请实施例提供的另一种训练模型的方法的流程示意图。如图 9 所示，本申请提供的另一种训练模型的方法，可以包括以下步骤：

1001、第一端侧设备获取训练数据集。

第一端侧设备可以获取样本数据集，样本数据集包括多个样本，多个样本中的每个样本均包括第一标签。样本数据集中的每个样本被预先标定有隐私级别，可以将需要隐私保护的样本划分一组，将不需要隐私保护的样本为另一组。比如需要隐私保护的样本为第一组样本数据集，不需要隐私保护的样本为第二组样本数据集。

1002、第一端侧设备通过样本数据集中的不需要隐私保护的数据对初始的共享模型进行训练，通过样本数据集中的需要隐私保护的数据和不需要隐私保护的数据对初始的私有模型进行训练。

由于初始的共享模型要参与到联邦学习和融合的过程，因此出于保护隐私的考虑，仅采用样本数据集中的不需要隐私保护的数据对初始的共享模型进行训练，而不采用需要隐私保护的数据对初始的共享模型进行训练，即仅采用第二组样本数据集对初始的共享模型进行训练。关于初始的共享模型可以参照图 8 对应的实施例中的步骤 901 中关于初始的共享模型的描述进行理解，这里不再重复赘述。

由于私有模型不直接参与联邦学习和融合的过程，仅在端侧设备进行存储和训练，所以以第一组样本数据集和第二组样本数据集均可以对初始的私有模型进行训练。

将第二组样本数据集输入到初始的共享模型后，初始的共享模型的特征提取模型可以提取样本的特征，并将样本的特征传输至初始的共享模型的任务模型，以输出预测结果，根据预测结果和第一标签的差异确定第一损失值。

将第一组样本数据集和第二组样本数据集输入到初始的私有模型后，初始的私有模型的特征提取模型可以提取样本的特征，并将样本的特征传输至初始的私有模型的任务模型，以输出预测结果，根据预测结果和第一标签的差异确定第二损失值。

通过对第一损失值和第二损失值进行融合处理可以获取第三损失值，根据第三损失值和结合梯度优化方法可以更新初始的私有模型和初始的共享模型，具体的可以更新初始的私有模型的特征提取模型的权重参数和初始的私有模型的任务模型的权重参数，以得到训练后的私有模型，还可以更新初始的共享模型的特征提取模型的权重参数和初始的共享模型的任务模型的权重参数。

1003、第一端侧设备向服务器发送第一共享模型。

1004、服务器根据至少两个端侧设备发送的第一共享模型进行融合处理，以获取第二

共享模型。

1005、第一端侧设备接收服务器发送的第二共享模型。

步骤 1003 至步骤 1005 可以参照图 8 对应的实施例中的步骤 901 至步骤 903 进行理解，这里不再重复赘述。

5 1006、通过第二共享模型输出针对第二组训练数据集的第一预测结果。

1007、第一端侧设备根据第一预测结果获取第一损失值。

1008、第一端侧设备通过第一私有模型输出针对第一组训练数据集和第二组训练数据集的第二预测结果。

1009、第一端侧设备根据第二预测结果获取第二损失值。

10 1010、第一端侧设备对第一损失值和第二损失值进行第二融合处理，以获取第三损失值，第三损失值用于更新私有模型。

在一个可能的实施方式中，还可以步骤 1011、向服务器发送第三共享模型。

针对于步骤 1011，还可以包括步骤 1012、服务器根据第三共享模型更新第二共享模型。

15 步骤 1006 可以参照图 8 对应的实施例中的步骤 904 进行理解。步骤 1007 至步骤 1012 可以参照图 8 对应的实施例中的步骤 905 至步骤 910 进行理解，这里不再重复赘述。

由图 9 对应的实施例可知，针对一些端侧设备可能对数据的隐私保护有很高的需求的场景，可以对端侧设备的训练数据按照需要隐私保护的高低进行划分，其中对隐私保护要求高的数据仅参与私有模型的训练过程，其余的数据可以既参与共享模型的训练过程也参与私有模型的训练过程。

20 以上对本申请提供的一种模型的训练的方法进行了介绍，通过本申请训练得到的私有模型可以用于执行推理任务，比如可以用于执行分类任务，回归任务等等，本申请实施例对此并不进行限定。下面对本申请提供的一种数据处理的方法进行具体的介绍。

参照图 10，为本申请提供的一种数据处理方法的流程示意图。

本申请提供的一种数据处理方法可以包括以下步骤：

25 1101、获取待处理数据。

本申请中的待处理数据可以是图像数据，文本数据，语音数据，视频数据等等。

1102、根据端侧设备存储的目标模型对待处理数据进行处理，以获取预测结果。

通过目标模型的特征提取模型提取待处理数据的特征，并将提取出的特征输入至目标模型的任务模型，以通过任务模型输出预测结果。

30 目标模型可以是上述图 8 或图 9 所描述的一种训练模型的方法训练得到的模型。

在一个可能的实施方式中，目标模型是通过第三损失值更新第一私有模型获取的，第三损失值是对第一损失值和第二损失值进行第二融合处理后获取的，第一损失值是通过第一预测结果获取的，第一预测结果是第二共享模型输出的针对训练数据集的预测结果，第二共享模型是从服务器中获取的，第二模型是服务器对至少两个端侧发送的第一共享模型进行第一融合处理后获取的，第二损失值是通过第二预测结果获取的，第二预测结果是第一私有模型输出的针对训练数据集的预测结果。由第二方面可知，本申请提供的方案，目标模型是通过共享模型学习到的知识以及本地训练数据集训练得到的模型，相比于现有技

35

术中端侧设备训练得到的模型，本申请中的目标模型性能更优。

在一个可能的实施方式中，第二共享模型包括第一特征提取模型，私有模型包括第二特征提取模型和第一任务模型，第一特征提取模型用于第一端侧设备接收到服务器发送的第二共享模型后，将第二特征提取模型更新为第一特征提取模型，第三损失值用于更新第一特征提取模型和第一任务模型，目标模型包括更新后的第一特征提取模型和更新后的第一任务模型。

在一个可能的实施方式中，所述第三损失值还用于更新所述第二共享模型，以得到第三共享模型，所述第三共享模型用于发送至所述服务器，以使所述服务器更新所述第二共享模型。

在一个可能的实施方式中，所述第一损失值包括交叉熵损失值和双向蒸馏损失值中的一个或者多个，所述第二损失值包括交叉熵损失值和双向蒸馏损失值中的一个或者多个。

在一个可能的实施方式中，所述训练数据集包括第一训练数据集和第二训练数据集，所述第一训练数据集预先设定需要隐私保护，所述第二训练数据集预先设定不需要隐私保护，所述第一预测结果是所述第二共享模型输出的针对所述第二训练数据集的预测结果，所述第二预测结果是所述第一私有模型输出的针对所述第一训练数据集和所述第二训练数据集的预测结果。

在一个可能的实施方式中，所述第三损失值是通过所述对所述第一损失值和所述第二损失值进行加权处理后获取的。

在一个可能的实施方式中，所述第三损失值具体是通过所述对所述第一损失值和所述第二损失值进行求平均值处理后获取的。

以上对本申请提供的一种训练模型的方法以及数据处理的方法进行了介绍，通过本申请实施例提供的方案，根据本地存储的训练数据以及共享模型在联邦学习过程中学习到的知识更新私有模型，使得训练得到的模型性能更优。可以理解的是，上述端侧设备为了实现上述功能，其包含了执行各个功能相应的硬件结构和/或软件模块。本领域技术人员应该很容易意识到，结合本文中所公开的实施例描述的各示例的模块及算法步骤，本申请能够以硬件或硬件和计算机软件的结合形式来实现。某个功能究竟以硬件还是计算机软件驱动硬件的方式来执行，取决于技术方案的特定应用和设计约束条件。专业技术人员可以对每个特定的应用来使用不同方法来实现所描述的功能，但是这种实现不应认为超出本申请的范围。

从硬件结构上来描述，图 8 至图 10 中的端侧设备可以由一个实体设备实现，也可以由多个实体设备共同实现，还可以是一个实体设备内的一个逻辑功能模块，本申请实施例对此不作具体限定。下面基于前述的训练模型的方法以及数据处理的方法，对本申请提供的端侧设备进行阐述，端侧设备用于执行前述图 8-10 对应的方法的步骤，或者端侧设备用于执行前述图 10 对应的方法的步骤。

例如，端侧设备可以通过图 11 中的计算机设备来实现，图 11 所示为本申请实施例提供的端侧设备的硬件结构示意图。包括：通信接口 1201 和处理器 1202，还可以包括存储器 1203。

通信接口 1201 可以使用任何收发器一类的装置,用于与其他设备或通信网络通信,在本方案中,端侧设备可以利用通信接口 1201 与服务器进行通信,比如上传模型或者下载模型。在一个可能的实施方式中,通信接口 1201 可以采用以太网,无线接入网 (radio access network, RAN), 无线局域网 (wireless local area networks, WLAN) 等技术与服务

5 进行通信。在一个可能的实施方式中,参照图 12,端侧设备由多个实体设备共同实现时,可以将通信接口看做传输设备,比如可以将通信接口看做网关、交换机、无线路由等计算机通讯设备。

处理器 1202 包括但不限于中央处理器 (central processing unit, CPU), 网络处理器 (network processor, NP), 专用集成电路 (application-specific integrated circuit, ASIC) 或者可编程逻辑器件 (programmable logic device, PLD) 中的一个或多个。上述 PLD 可以是复杂可编程逻辑器件 (complex programmable logic device, CPLD), 现场可编程逻辑门阵列 (field-programmable gate array, FPGA), 通用阵列逻辑 (generic array logic, GAL) 或其任意组合。处理器 1202 负责通信线路 1204 和通常的处理,还可以提供各种功能,包括定时,外围接口,电压调节,电源管理以及其他控制功能。

15 参照图 12,端侧设备由多个实体设备共同实现时,可以将处理器看做运算设备,可以将与处理器看做包括处理器 1202 的运算组件。存储器 1203 可以用于存储处理器 1202 在执行操作时所使用的数据。

存储器 1203 可以是只读存储器 (read-only memory, ROM) 或可存储静态信息和指令的其他类型的静态存储设备,随机存取存储器 (random access memory, RAM) 或者可存储信息和指令的其他类型的动态存储设备,也可以是电可擦可编程只读存储器 (electrically eraser server able programmable read-only memory, EEPROM)、只读光盘 (compact disc read-only memory, CD-ROM) 或其他光盘存储、光碟存储 (包括压缩光碟、激光碟、光碟、数字通用光碟、蓝光光碟等)、磁盘存储介质或者其他磁存储设备、或者能够用于携带或存储具有指令或数据结构形式的期望的程序代码并能够由计算机存取的任何其他介质,但

20 不限于此。存储器可以是独立存在,通过通信线路 1204 与处理器 1202 相连接。存储器 1203 也可以和处理器 1202 集成在一起。如果存储器 1203 和处理器 1202 是相互独立的器件,存储器 1203 和处理器 1202 相连,例如存储器 1203 和处理器 1202 可以通过通信线路通信。通信接口 1201 和处理器 1202 可以通过通信线路通信,通信接口 1201 也可以与处理器 1202 直连。

30 通信线路 1204 可以包括任意数量的互联的总线和桥,通信线路 1204 将包括由处理器 1202 代表的一个或多个处理器 1202 和存储器 1203 代表的存储器的各种电路链接在一起。通信线路 1204 还可以将诸如外围设备、稳压器和功率管理电路等之类的各种其他电路链接在一起,这些都是本领域所公知的,因此,本申请不再对其进行进一步描述。

在一个具体的实施方式中,该端侧设备,可以包括:存储器,用于存储计算机可读指令。还可以包括和存储器耦合的通信接口和处理器。通信接口用于执行图 8 对应的实施例中的步骤 900、步骤 901、步骤 903 以及步骤 909。处理器用于执行所述存储器中的计算机可读指令从而执行图 8 对应的实施例中的步骤 904 至步骤 908。

35

在一个具体的实施方式中，该端侧设备，可以包括：存储器，用于存储计算机可读指令。还可以包括和存储器耦合的通信接口和处理器。通信接口用于执行图 9 对应的实施例中的步骤 1011、步骤 1003、步骤 1005 以及步骤 1011。处理器用于执行所述存储器中的计算机可读指令从而执行图 9 对应的实施例中的步骤 1002，步骤 1006 至步骤 1010。

5 在一个可能的实施方式中，该端侧设备，可以包括存储器，用于存储计算机可读指令。还可以包括和存储器耦合的通信接口和处理器。通信接口用于执行图 10 中的步骤 1101，处理器用于执行图 10 对应的实施例中的步骤 1102。

在本申请实施例中，可以将通信接口视为端侧设备的收发模块 1401，将具有处理功能的处理器视为端侧设备的训练模块 1402，将存储器视为端侧设备的存储模块（图中未示出）。
10 参阅图 13，为本申请实施例提供的一种端侧设备的结构示意图。

在本申请实施例中，还可以将通信接口视为端侧设备的收发模块 1501，将具有处理功能的处理器视为端侧设备的推理模块 1502，将存储器视为端侧设备的存储模块（图中未示出）。参阅图 14，为本申请实施例提供的另一种端侧设备的结构示意图。

继续参阅图 12，为本申请实施例提供方案的一种可能的应用场景示意图。企业拥有的
15 数据一般都有巨大的潜在价值，但是出于隐私性考虑，企业之间的数据往往不能够简单的交换。此外，不同企业拥有的数据分布往往具有很大的差异。为了解决这些问题，企业会加入联邦学习系统，共同组建模型。每一个企业可以看做拥有一个端侧设备，该端侧设备可以理解为一个设备或者多个设备的组合。比如参照图 12，该端侧设备可能包括运算设备和传输设备。其中运算设备执行的过程可以参照上文提到的处理器进行理解，传输设备
20 执行的过程可以参照上文提到的通信接口进行理解，这里不再重复赘述。各个端侧设备和服务器之间的交互过程可以参照图 8 以及图 9 对应的实施例进行理解，这里不再重复赘述。

应当理解，上述仅为本申请实施例提供的一个例子，并且，端侧设备可具有比示出的部件更多或更少的部件，可以组合两个或更多个部件，或者可具有部件的不同配置实现。

25 在上述实施例中，可以全部或部分地通过软件、硬件、固件或者其任意组合来实现。当使用软件实现时，可以全部或部分地以计算机程序产品的形式实现。

本申请实施例提供的端侧设备可以为芯片，芯片包括：处理单元和通信单元，所述处理单元例如可以是处理器，所述通信单元例如可以是输入/输出接口、管脚或电路等。该处理单元可执行存储单元存储的计算机执行指令，以使芯片执行上述图 8 或图 9 所示实施例描述的训练模型的方法。在另一个可能的实施方式中，以使芯片执行上述图 10 所示实施例描述的数据处理的方法。可选地，所述存储单元为所述芯片内的存储单元，如寄存器、缓存等，所述存储单元还可以是所述无线接入设备端内的位于所述芯片外部的存储单元，如只读存储器（read-only memory, ROM）或可存储静态信息和指令的其他类型的静态存储设备，随机存取存储器（random access memory, RAM）等。

35 具体地，前述的处理单元或者处理器可以是中央处理器（central processing unit, CPU）、网络处理器（neural-network processing unit, NPU）、图形处理器（graphics processing unit, GPU）、数字信号处理器（digital signal processor, DSP）、专用集

成电路 (application specific integrated circuit, ASIC) 或现场可编程逻辑门阵列 (field programmable gate array, FPGA) 或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件等。通用处理器可以是微处理器或者也可以的任何常规的处理器等。

5 具体的, 请参阅图 15, 图 15 为本申请实施例提供的芯片的一种结构示意图, 所述芯片可以表现为神经网络处理器 NPU160, NPU160 作为协处理器挂载到主 CPU (Host CPU) 上, 由 Host CPU 分配任务。NPU 的核心部分为运算电路 1603, 通过控制器 1604 控制运算电路 1603 提取存储器中的矩阵数据并进行乘法运算。

10 在一些实现中, 运算电路 1603 内部包括多个处理单元 (process engine, PE)。在一些实现中, 运算电路 1603 是二维脉动阵列。运算电路 1603 还可以是一维脉动阵列或者能够执行例如乘法和加法这样的数学运算的其它电子线路。在一些实现中, 运算电路 1603 是通用的矩阵处理器。

举例来说, 假设有输入矩阵 A, 权重矩阵 B, 输出矩阵 C。运算电路从权重存储器 1602 中取矩阵 B 相应的数据, 并缓存在运算电路中每一个 PE 上。运算电路从输入存储器 1601 15 中取矩阵 A 数据与矩阵 B 进行矩阵运算, 得到的矩阵的部分结果或最终结果, 保存在累加器 (accumulator) 1608 中。

统一存储器 1606 用于存放输入数据以及输出数据。权重数据直接通过存储单元访问控制器 (direct memory access controller, DMAC) 1605, DMAC 被搬运到权重存储器 1602 中。输入数据也通过 DMAC 被搬运到统一存储器 1606 中。

20 总线接口单元 (bus interface unit, BIU) 1610, 用于 AXI 总线与 DMAC 和取指存储器 (Instruction Fetch Buffer, IFB) 1609 的交互。

总线接口单元 1610 (bus interface unit, BIU), 用于取指存储器 1609 从外部存储器获取指令, 还用于存储单元访问控制器 1605 从外部存储器获取输入矩阵 A 或者权重矩阵 B 的原数据。

25 DMAC 主要用于将外部存储器 DDR 中的输入数据搬运到统一存储器 1606 或将权重数据搬运到权重存储器 1602 中或将输入数据数据搬运到输入存储器 1601 中。

向量计算单元 1607 包括多个运算处理单元, 在需要的情况下, 对运算电路的输出做进一步处理, 如向量乘, 向量加, 指数运算, 对数运算, 大小比较等等。主要用于神经网络中非卷积/全连接层网络计算, 如批归一化 (batch normalization), 像素级求和, 对特征平面进行上采样等。

30 在一些实现中, 向量计算单元 1607 能将经处理的输出的向量存储到统一存储器 1606。例如, 向量计算单元 1607 可以将线性函数和/或非线性函数应用到运算电路 1603 的输出, 例如对卷积层提取的特征平面进行线性插值, 再例如累加值的向量, 用以生成激活值。在一些实现中, 向量计算单元 1607 生成归一化的值、像素级求和的值, 或二者均有。在 35 一些实现中, 处理过的输出的向量能够用作到运算电路 1603 的激活输入, 例如用于在神经网络中的后续层中的使用。

控制器 1604 连接的取指存储器 (instruction fetch buffer) 1609, 用于存储控制器

1604 使用的指令。

统一存储器 1606, 输入存储器 1601, 权重存储器 1602 以及取指存储器 1609 均为 On-Chip 存储器。外部存储器私有于该 NPU 硬件架构。

其中, 循环神经网络中各层的运算可以由运算电路 1603 或向量计算单元 1607 执行。

5 其中, 上述任一处提到的处理器, 可以是一个通用中央处理器, 微处理器, ASIC, 或一个或多个用于控制上述图 8 或图 9 的方法的程序执行的集成电路, 或者在另一个可能的实施方式中, 控制上述图 10 的方法的程序执行的集成电路。

另外需说明的是, 以上所描述的装置实施例仅仅是示意性的, 其中所述作为分离部件说明的单元可以是或者也可以不是物理上分开的, 作为单元显示的部件可以是或者也可以不是物理单元, 即可以位于一个地方, 或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部模块来实现本实施例方案的目的。另外, 本申请提供的装置实施例附图中, 模块之间的连接关系表示它们之间具有通信连接, 具体可以实现为一条或多条通信总线或信号线。

通过以上的实施方式的描述, 所属领域的技术人员可以清楚地了解到本申请可借助软件+加必需的通用硬件的方式来实现, 当然也可以通过专用硬件包括专用集成电路、专用 CPU、专用存储器、专用元器件等来实现。一般情况下, 凡由计算机程序完成的功能都可以很容易地用相应的硬件来实现, 而且, 用来实现同一功能的具体硬件结构也可以是多种多样的, 例如模拟电路、数字电路或专用电路等。但是, 对本申请而言更多情况下软件程序实现是更佳的实施方式。基于这样的理解, 本申请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可读取的存储介质中, 如计算机的软盘、U 盘、移动硬盘、只读存储器 (read only memory, ROM)、随机存取存储器 (random access memory, RAM)、磁碟或者光盘等, 包括若干指令用以使得一台计算机设备 (可以是个人计算机, 服务器, 或者网络设备等) 执行本申请各个实施例所述的方法。

25 在上述实施例中, 可以全部或部分地通过软件、硬件、固件或者其任意组合来实现。当使用软件实现时, 可以全部或部分地以计算机程序产品的形式实现。

本申请实施例中还提供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用于训练模型的程序, 当其在计算机上运行时, 使得计算机执行如前述图 8 或图 9 所示实施例描述的方法中的步骤。

30 本申请实施例中还提供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用于数据处理的程序, 当其在计算机上运行时, 使得计算机执行如前述图 10 所示实施例描述的方法中的步骤。

本申请实施例还提供一种数字处理芯片。该数字处理芯片中集成了用于实现上述处理器, 或者处理器的功能的电路和一个或者多个接口。当该数字处理芯片中集成了存储器时, 35 该数字处理芯片可以完成前述实施例中的任一个或多个实施例的方法步骤。当该数字处理芯片中未集成存储器时, 可以通过通信接口与外置的存储器连接。该数字处理芯片根据外置的存储器中存储的程序代码来实现上述实施例中端侧设备执行的动作。

本申请实施例中还提供一种计算机程序产品，所述计算机程序产品包括一个或多个计算机指令。在计算机上加载和执行所述计算机程序指令时，全部或部分地产生按照本申请实施例所述的流程或功能。所述计算机可以是通用计算机、专用计算机、计算机网络、或者其他可编程装置。所述计算机指令可以存储在计算机可读存储介质中，或者从一个计算机可读存储介质向另一计算机可读存储介质传输，例如，所述计算机指令可以从一个网站站点、计算机、服务器或数据中心通过有线（例如同轴电缆、光纤、数字用户线（DSL））或无线（例如红外、无线、微波等）方式向另一个网站站点、计算机、服务器或数据中心进行传输。所述计算机可读存储介质可以是计算机能够存储的任何可用介质或者是包含一个或多个可用介质集成的服务器、数据中心等数据存储设备。所述可用介质可以是磁性介质，（例如，软盘、硬盘、磁带）、光介质（例如，DVD）、或者半导体介质（例如固态硬盘 Solid State Disk(SSD)）等。

本领域普通技术人员可以理解上述实施例的各种方法中的全部或部分步骤是可以通程序来指令相关的硬件来完成，该程序可以存储于一计算机可读存储介质中，存储介质可以包括：ROM、RAM、磁盘或光盘等。

以上对本申请实施例所提供的模型的训练方法、数据处理方法以及相关设备进行了详细介绍，本文中应用了具体个例对本申请的原理及实施方式进行了阐述，以上实施例的说明只是用于帮助理解本申请的方法及其核心思想；同时，对于本领域的一般技术人员，依据本申请的思想，在具体实施方式及应用范围上均会有改变之处，综上所述，本说明书内容不应理解为对本申请的限制。

本申请的说明书和权利要求书及上述附图中的术语“第一”，“第二”等是用于区别类似的对象，而不必用于描述特定的顺序或先后次序。应该理解这样使用的数据在适当情况下可以互换，以便这里描述的实施例能够以除了在这里图示或描述的内容以外的顺序实施。本申请中术语“和/或”，仅仅是一种描述关联对象的关联关系，表示可以存在三种关系，例如，A 和/或 B，可以表示：单独存在 A，同时存在 A 和 B，单独存在 B 这三种情况，另外，本文中字符“/”，一般表示前后关联对象是一种“或”的关系。此外，术语“包括”和“具有”以及他们的任何变形，意图在于覆盖不排他的包含，例如，包含了一系列步骤或模块的过程，方法，系统，产品或设备不必限于清楚地列出的那些步骤或模块，而是可包括没有清楚地列出的或对于这些过程，方法，产品或设备固有的其它步骤或模块。在本申请中出现的对步骤进行的命名或者编号，并不意味着必须按照命名或者编号所指示的时间/逻辑先后顺序执行方法流程中的步骤，已经命名或者编号的流程步骤可以根据要实现的技术目的变更执行次序，只要能达到相同或者相类似的技术效果即可。本申请中所出现的模块的划分，是一种逻辑上的划分，实际应用中实现时可以有另外的划分方式，例如多个模块可以结合成或集成在另一个系统中，或一些特征可以忽略，或不执行，另外，所显示的或讨论的相互之间的耦合或直接耦合或通信连接可以是通过一些端口，模块之间的间接耦合或通信连接可以是电性或其他类似的形式，本申请中均不作限定。并且，作为分离部件说明的模块或子模块可以是也可以不是物理上的分离，可以是也可以不是物理模块，或者可以分布到多个电路模块中，可以根据实际的需要选择其中的部分或全

部模块来实现本申请方案的目的。

权 利 要 求

- 1、一种训练模型的方法，其特征在于，所述方法适用于机器学习系统，所述机器学习系统包括服务器和至少两个端侧设备，针对第一端侧设备，所述第一端侧设备是所述至少两个端侧中的任意一个端侧设备，所述方法包括：
- 5 接收所述服务器发送的第一共享模型；
通过所述第一共享模型输出针对数据集的第一预测结果；
根据所述第一预测结果获取第一损失值；
通过所述第一端侧设备的第一私有模型输出针对所述数据集的第二预测结果；
根据所述第二预测结果获取第二损失值；
- 10 对所述第一损失值和所述第二损失值进行融合处理，以获取第三损失值，所述第三损失值用于更新所述第一私有模型。
- 2、根据权利要求1所述的方法，其特征在于，所述第一共享模型和所述第一私有模型共享特征提取模型。
- 3、根据权利要求2所述的方法，其特征在于，接收所述第一共享模型之前，所述第一终端设备存储有第二私有模型，所述方法还包括：
- 15 根据所述第一共享模型的特征提取模型更新所述第二私有模型的特征提取模型，以得到所述第一私有模型。
- 4、根据权利要求1至3任一项所述的方法，其特征在于，所述第三损失值还用于更新所述第一共享模型，以得到第二共享模型，所述方法还包括：
- 20 向所述服务器发送所述第二共享模型，所述第二共享模型用于所述服务器更新所述第一共享模型。
- 5、根据权利要求1至4任一项所述的方法，其特征在于，所述第一损失值包括交叉熵损失值和双向蒸馏损失值中的至少一个，所述第二损失值包括交叉熵损失值和双向蒸馏损失值中的至少一个。
- 25 6、根据权利要求1至5任一项所述的方法，其特征在于，所述数据集包括需要隐私保护的第一数据集和不需要隐私保护的第二个数据集，
所述通过所述第一共享模型输出针对数据集的第一预测结果，包括：
通过所述第一共享模型输出针对所述第二数据集的第一预测结果；
所述通过所述第一端侧设备的第一私有模型输出针对所述数据集的第二预测结果，包
- 30 括：
通过所述第一私有模型输出针对所述第一数据集和第二数据集的第二预测结果。
- 7、根据权利要求1至6任一项所述的方法，其特征在于，所述对所述第一损失值和所述第二损失值进行融合处理，以获取第三损失值，包括：
- 对所述第一损失值和所述第二损失值进行加权处理，以获取所述第三损失值。
- 35 8、根据权利要求7所述的方法，其特征在于，所述第一损失值和所述第二损失值进行加权处理，以获取所述第三损失值，包括：
对所述第一损失值和所述第二损失值进行求平均值处理，以获取所述第三损失值。
- 9、一种数据处理的方法，其特征在于，所述方法适用于机器学习系统，所述机器学习

系统包括服务器和至少两个端侧设备，针对第一端侧设备，所述第一端侧设备是所述至少两个端侧中的任意一个端侧设备，所述方法包括：

获取待处理数据；

根据所述第一端侧设备存储的目标模型对所述待处理数据进行处理，以获取预测结果，其中，所述目标模型是通过第三损失值更新第一私有模型获取的，所述第三损失值是对第一损失值和第二损失值进行融合处理后获取的，所述第一损失值是通过第一预测结果获取的，所述第一预测结果是第一共享模型输出的针对数据集的预测结果，所述第一共享模型是从服务器中获取的，所述第二损失值是通过第二预测结果获取的，所述第二预测结果是第一私有模型输出的针对数据集的预测结果。

10、根据权利要求9所述的方法，其特征在于，所述第一共享模型和所述第一私有模型共享特征提取模型。

11、根据权利要求10所述的方法，其特征在于，接收所述第一共享模型之前，所述第一终端设备存储有第二私有模型，所述第一私有模型是根据所述第一共享模型的特征提取模型更新所述第二私有模型的特征提取模型后获取的。

12、根据权利要求9至11所述的方法，其特征在于，所述第三损失值还用于更新所述第一共享模型，以得到第二共享模型，所述第二共享模型用于发送至所述服务器，以使所述服务器更新所述第一共享模型。

13、根据权利要求9至12任一项所述的方法，其特征在于，所述第一损失值包括交叉熵损失值和双向蒸馏损失值中的至少一个，所述第二损失值包括交叉熵损失值和双向蒸馏损失值中的至少一个。

14、根据权利要求9至13任一项所述的方法，其特征在于，所述数据集包括需要隐私保护的第一数据集和不需要隐私保护的第二数据集，所述第一预测结果是所述第一共享模型输出的针对所述第二数据集的预测结果，所述第二预测结果是所述第一私有模型输出的针对所述第一数据集和所述第二数据集的预测结果。

15、根据权利要求9至14任一项所述的方法，其特征在于，所述第三损失值是通过所述第一损失值和所述第二损失值进行加权处理后获取的。

16、根据权利要求15所述的方法，其特征在于，所述第三损失值具体是通过所述第一损失值和所述第二损失值进行求平均值处理后获取的。

17、一种端侧设备，其特征在于，所述端侧设备适用于机器学习系统，所述机器学习系统包括至少两个端侧设备，针对第一端侧设备，所述第一端侧设备是所述至少两个端侧中的任意一个端侧设备，包括收发模块和训练模块，

所述收发模块，用于接收服务器发送的所述第一共享模型；

所述训练模块，用于：

通过所述第一共享模型输出针对数据集的第一预测结果；

根据所述第一预测结果获取第一损失值；

通过所述第一端侧设备的第一私有模型输出针对所述数据集的第二预测结果；

根据所述第二预测结果获取第二损失值；

对所述第一损失值和所述第二损失值进行融合处理，以获取第三损失值，所述第三损失值用于更新所述第一私有模型。

18、根据权利要求 17 所述的端侧设备，其特征在于，所述第一共享模型和所述第一私有模型共享特征提取模型。

5 19、根据权利要求 18 所述的端侧设备，其特征在于，接收所述第一共享模型之前，所述第一终端设备存储有第二私有模型，所述训练模块还用于：

根据所述第一共享模型的特征提取模型更新所述第二私有模型的特征提取模型，以得到所述第一私有模型。

20、根据权利要求 17 至 19 任一项所述的端侧设备，其特征在于，所述第三损失值还用于更新所述第一共享模型，以得到第二共享模型，所述收发模块，还用于：

向所述服务器发送所述第二共享模型，所述第二共享模型用于所述服务器更新所述第一共享模型。

21、根据权利要求 17 至 20 任一项所述的端侧设备，其特征在于，所述第一损失值包括交叉熵损失值和双向蒸馏损失值中的至少一个，所述第二损失值包括交叉熵损失值和双向蒸馏损失值中的至少一个。

22、根据权利要求 17 至 21 任一项所述的端侧设备，其特征在于，所述数据集包括需要隐私保护的第一数据集和不需要隐私保护的第二数据集，

所述训练模块，具体用于通过所述第一共享模型输出针对所述第二数据集的第一预测结果；

20 所述训练模块，具体用于通过所述第一端侧设备的第一私有模型输出针对所述第一数据集和第二数据集的第二预测结果。

23、根据权利要求 17 至 22 任一项所述的端侧设备，其特征在于，所述训练模块具体用于：

对所述第一损失值和所述第二损失值进行加权处理，以获取所述第三损失值。

25 24、根据权利要求 23 所述的端侧设备，其特征在于，所述训练模块具体用于：

对所述第一损失值和所述第二损失值进行求平均值处理，以获取所述第三损失值。

25、一种端侧设备，其特征在于，所述端侧设备适用于机器学习系统，所述机器学习系统包括至少两个端侧设备，针对第一端侧设备，所述第一端侧设备是所述至少两个端侧中的任意一个端侧设备，包括：

30 获取模块，用于获取待处理数据；

推理模块，用于根据所述端侧设备存储的目标模型对所述待处理数据进行处理，以获取预测结果，其中，所述目标模型是通过第三损失值更新第一私有模型获取的，所述第三损失值是对第一损失值和第二损失值进行融合处理后获取的，所述第一损失值是通过第一预测结果获取的，所述第一预测结果是第一共享模型输出的针对数据集的预测结果，所述
35 第一共享模型是从服务器中获取的，所述第二损失值是通过第二预测结果获取的，所述第二预测结果是第一私有模型输出的针对数据集的预测结果。

26、一种机器学习系统，其特征在于，所述机器学习系统包括服务器和至少两个端侧

- 设备, 所述第一端侧设备是所述至少两个端侧中的任意一个端侧设备,
所述服务器, 用于向所述第一端侧设备发送第一共享模型;
所述第一端侧设备, 用于:
通过所述第一共享模型输出针对数据集的第一预测结果;
5 根据所述第一预测结果获取第一损失值;
通过所述第一端侧设备的第一私有模型输出针对所述数据集的第二预测结果;
根据所述第二预测结果获取第二损失值;
对所述第一损失值和所述第二损失值进行融合处理, 以获取第三损失值, 所述第三损失值用于更新所述第一私有模型。
- 10 27、一种端侧设备, 其特征在于, 包括:
存储器, 用于存储计算机可读指令;
还包括, 与所述存储器耦合的处理器, 用于执行所述存储器中的计算机可读指令从而执行如权利要求 1 至 8 任一项所描述的方法。
- 15 28、一种端侧设备, 其特征在于, 包括:
存储器, 用于存储计算机可读指令;
还包括, 与所述存储器耦合的处理器, 用于执行所述存储器中的计算机可读指令从而执行如权利要求 9 至 16 任一项所描述的方法。
- 20 29、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指令, 当指令在计算机装置上运行时, 使得所述计算机装置执行如权利要求 1 至 8 任一项所描述的方法。
- 30 30、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指令, 当指令在计算机装置上运行时, 使得所述计算机装置执行如权利要求 9 至 16 任一项所描述的方法。
- 25 31、一种计算机程序产品, 当所述计算机程序产品在计算机上运行时, 使得计算机可以执行如权利要求 1 至 8 任一所描述的方法。
- 32、一种计算机程序产品, 当所述计算机程序产品在计算机上运行时, 使得计算机可以执行如权利要求 9 至 16 任一所描述的方法。
- 33、一种芯片, 其特征在于, 所述芯片与存储器耦合, 用于执行所述存储器中存储的程序, 以执行如权利要求 1 至 8 任一项所述的方法。
- 30 34、一种芯片, 其特征在于, 所述芯片与存储器耦合, 用于执行所述存储器中存储的程序, 以执行如权利要求 9 至 16 任一项所述的方法。