(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2022 年 1 月 27 日 (27.01.2022)

WIPO | PCT

(10) 国际公布号
WO 2022/016964 A1

(51) 国际专利分类号:
G06N 20/00 (2019.01)

(21) 国际申请号: PCT/CN2021/093407

(22) 国际申请日: 2021 年 5 月 12 日 (12.05.2021)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
202010719397.5 2020年7月23日 (23.07.2020) CN

(71) 申请人: 深圳前海微众银行股份有限公司 (WEBANK CO., LTD) [CN/CN]; 中国广东省深圳市南山区沙河西路1819号深圳湾科技生态园7栋A座, Guangdong 518000 (CN)。

(72) 发明人: 何元钦 (HE, Yuanqin); 中国广东省深圳市南山区沙河西路1819号深圳湾科技生态园7栋A座, Guangdong 518000 (CN)。 梁新乐 (LIANG, Xinle); 中国广东省深圳市南山区沙河西路1819号深圳湾科技生态园7栋A座, Guangdong 518000 (CN)。 刘洋 (LIU, Yang); 中国广东省深圳市南山区沙河西路1819号深圳湾科技生态园7栋A座, Guangdong 518000 (CN)。 陈天健 (CHEN, Tianjian); 中国广东省深圳市南山区沙河西路1819号深圳湾科技生态园7栋A座, Guangdong 518000 (CN)。

(74) 代理人: 深圳市世纪恒程知识产权代理事务所 (CENFO INTELLECTUAL PROPERTY AGENCY); 中国广东省深圳市南山区西丽街道松坪山社区松坪山路3号奥特迅电力大厦201, Guangdong 518052 (CN)。

(81) 指定国 (除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK,

(54) **Title:** VERTICAL FEDERATED MODELING OPTIMIZATION METHOD AND DEVICE, AND READABLE STORAGE MEDIUM

(54) **发明名称**: 纵向联邦建模优化方法、设备及可读存储介质

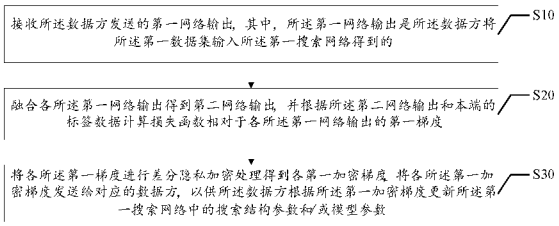

图 2

S10 Receive first network outputs sent by the data party, the first network outputs being obtained by inputting, by the data party, the first dataset into the first search network

S20 Fuse the first network outputs to obtain a second network output, and calculate a first gradient of a loss function relative to each first network output according to the second network output and tag data of a home terminal

S30 Perform differential privacy encryption processing on each first gradient to obtain first encryption gradients, and send each first encryption gradient to a corresponding data party, so that the data party updates a search structure parameter and/or a model parameter in the first search network according to the first encryption gradient

(57) **Abstract:** A vertical federated modeling optimization method and device, and a readable storage medium. The method comprises: receiving first network outputs sent by the data party, the first network outputs being obtained by inputting, by the data party, the first dataset into the first search network (S10); fusing the first network outputs to obtain a second network output, and calculating a first gradient of a loss function relative to each first network output according to the second network output and tag data of a home terminal (S20); and performing differential privacy encryption processing on each first gradient to obtain first encryption gradients, and sending each first encryption gradient to a corresponding data party, so that the data party updates a search structure parameter and/or a model parameter in the first search network according to the first encryption gradient (S30).

(57) **摘要**: 一种纵向联邦建模优化方法、设备及可读存储介质，所述方法包括：接收所述数据方发送的第一网络输出，其中，所述第一网络输出是所述数据方将所述第一数据集输入所述第一搜索网络得到的（S10）；融合各所述第一网络输出得到第二网络输出，并根据所述第二网络输出和本端的标签数据计算损失函数相对于各所述第一网络输出的第一梯度（S20）；将各所述第一梯度进行差分隐私加密处理得到各第一加密梯度，将各所述第一加密梯度发送给对应的数据方，以供所述数据方根据所述第一加密梯度更新所述第一搜索网络中的搜索结构参数和/或模型参数（S30）。

WO 2022/016964 A1

[见续页]

LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW。

(84) 指定国(除另有指明，要求每一种可提供的地区保护)：ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:

— 包括国际检索报告(条约第21条(3))。

纵向联邦建模优化方法、设备及可读存储介质

[0001] 本申请要求于2020年7月23日申请的、申请号为202010719397.5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。

技术领域

[0002] 本申请涉及人工智能技术领域，尤其涉及一种纵向联邦建模优化方法、设备及可读存储介质。

背景技术

[0003] 随着人工智能的发展，人们为解决数据孤岛的问题，提出了“联邦学习”的概念，使得联邦双方在不用给出己方数据的情况下，也可进行模型训练得到模型参数，并且可以避免数据隐私泄露的问题。

[0004] 纵向联邦学习是在参与者的数据特征重叠较小，而用户重叠较多的情况下，取出参与者用户相同而用户数据特征不同的那部分用户及数据进行联合训练机器学习模型。比如有属于同一个地区的两个参与者A和B，其中参与者A是一家银行，参与者B是一个电商平台。参与者A和B在同一地区拥有较多相同的用户，但是A与B的业务不同，记录的用户数据特征是不同的。特别地，A和B记录的用户数据特征可能是互补的。在这样的场景下，可以使用纵向联邦学习来帮助A和B构建联合机器学习预测模型，帮助A和B向他们的客户提供更好的服务。

[0005] 但是，目前纵向联邦学习的参与方在使用纵向联邦技术时需要对各自的模型结构进行预先的设计，而由于设计的模型结构稍有差别可能就会极大地影响整体纵向联邦学习技术的性能，使得纵向联邦学习的参与门槛较高，限制了纵向联邦学习在具体任务领域的应用范围。

发明概述

技术问题

[0006] 本申请的主要目的在于提供一种纵向联邦建模优化方法、设备及可读存储介质，旨在解决目前纵向联邦学习的参与方在使用纵向联邦技术时需要对各自的模型结构进行预先的设计，造成纵向联邦学习参与门槛高的问题。

问题的解决方案

技术解决方案

[0007] 为实现上述目的，本申请提供一种纵向联邦建模优化方法，所述方法应用于参与纵向联邦建模的标签方，所述标签方与参与纵向联邦建模的各数据方通信连接，各所述数据方中分别部署有基于各自数据特征构建的第一数据集和第一搜索网络，所述方法包括以下步骤：

[0008] 接收所述数据方发送的第一网络输出，其中，所述第一网络输出是所述数据方将所述第一数据集输入所述第一搜索网络得到的；

[0009] 融合各所述第一网络输出得到第二网络输出，并根据所述第二网络输出和本端的标签数据计算损失函数相对于各所述第一网络输出的第一梯度；

[0010] 将各所述第一梯度进行差分隐私加密处理得到各第一加密梯度，将各所述第一加密梯度发送给对应的数据方，以供所述数据方根据所述第一加密梯度更新所述第一搜索网络中的搜索结构参数和/或模型参数。

[0011] 为实现上述目的，本申请还提供一种纵向联邦建模优化方法，所述方法应用于参与纵向联邦建模的数据方，各数据方中分别部署有基于各自数据特征构建的第一数据集和第一搜索网络，所述方法包括以下步骤：

[0012] 将所述第一数据集输入所述第一搜索网络得到网络原始输出；

[0013] 对所述网络原始输出进行差分隐私加密处理得到第一网络输出；

[0014] 将所述第一网络输出发送给参与纵向联邦建模的标签方，以供所述标签方对从各数据方接收到的所述第一网络输出进行融合得到第二网络输出后，根据所述第二网络输出和所述标签方的标签数据计算损失函数相对于各所述第一网络输出的第一梯度，并将所述第一梯度并返回给对应的数据方；

[0015] 根据从所述标签方接收到的所述第一梯度更新所述第一搜索网络中的搜索结构参数和/或模型参数。

[0016] 为实现上述目的，本申请还提供一种纵向联邦建模优化设备，所述纵向联邦建模优化设备包括：存储器、处理器及存储在所述存储器上并可在所述处理器上运行的纵向联邦建模优化程序，所述纵向联邦建模优化程序被所述处理器执行时实现如上所述的纵向联邦建模优化方法的步骤。

[0017] 此外，为实现上述目的，本申请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纵向联邦建模优化程序，所述纵向联邦建模优化程序被处理器执行时实现如上所述的纵向联邦建模优化方法的步骤。

发明的有益效果

有益效果

[0018] 本申请中，通过标签方接收数据方发送的第一网络输出，其中，第一网络输出是所述数据方将所述第一数据集输入所述第一搜索网络得到的；标签方融合各第一网络输出得到第二网络输出，并根据第二网络输出和本端的标签数据计算损失函数相对于各第一网络输出的第一梯度；将各第一梯度进行差分隐私加密处理得到各第一加密梯度，将各第一加密梯度发送给对应的数据方，以供数据方根据第一加密梯度更新第一搜索网络中的搜索结构参数和/或模型参数。在本申请中，由于标签方发送给数据方的梯度是经过差分隐私加密处理后的，数据方无法获知原始的梯度，从而避免了数据方根据梯度推导出标签方的标签数据和特征数据，也就避免了标签方中的隐私数据泄露给数据方，提升了在纵向联邦建模过程中标签方的数据安全性。并且，相比于现有纵向联邦学习中，各参与方需要人工花费大量人力物力预先设计模型结构的方式，本申请实现了在纵向联邦建模过程中，数据方只需要设置各自的搜索网络即可，搜索网络中各个网络单元之间的连接，也即模型结构，是在纵向联邦建模过程中通过优化更新搜索结构参数的方式自动确定的，实现了自动纵向联邦学习，不需要花费大量人力物力预先设置模型结构，降低了参与纵向联邦学习的门槛，使得纵向联邦学习能够被应用于更广泛的具体任务领域中去实现具体的任务，提高了纵向联邦学习的应用范围。且建模过程中，数据方向标签方发送的是搜索网络的输出，标签方向数据方发送的是差分隐私处理后的梯度，各个参与方之间并不会直接交互数据集和模型本身，从而一定程度上保障了各个参与方的数据安全和模型信息安全。

对附图的简要说明

附图说明

[0019] 图1为本申请实施例方案涉及的硬件运行环境的结构示意图；

[0020] 图2为本申请纵向联邦建模优化方法第一实施例的流程示意图；

[0021] 图3为本申请实施例涉及的一种差分隐私加密通信信息的自动纵向联邦学习框架图。

发明实施例

本发明的实施方式

[0022] 应当理解，此处所描述的具体实施例仅仅用以解释本申请，并不用于限定本申请。

[0023] 如图1所示，图1是本申请实施例方案涉及的硬件运行环境的设备结构示意图。

[0024] 需要说明的是，本申请实施例纵向联邦建模优化设备可以是智能手机、个人计算机和服务器等设备，在此不做具体限制。

[0025] 如图1所示，该纵向联邦建模优化设备可以包括：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。

[0026] 本领域技术人员可以理解，图1中示出的设备结构并不构成对纵向联邦建模优化设备的限定，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。

[0027] 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、用户接口模块以及纵向联邦建模优化程序。其中，操作系统是管理和控制设备硬件和软件资源的程序，支持纵向联邦建模优化程序以及其它软件或程序的运行。

[0028] 当图1所示设备为参与纵向联邦建模的标签方时，在图1所示的设备中，用户接口1003主要用于与客户端进行数据通信；网络接口1004主要用于与参与纵向联邦建模的数据方建立通信连接，各数据方中分别部署有基于各自数据特征构建

的第一数据集和第一搜索网络；处理器1001可以用于调用存储器1005中存储的纵向联邦建模优化程序，并执行以下操作：

[0029] 接收所述数据方发送的第一网络输出，其中，所述第一网络输出是所述数据方将所述第一数据集输入所述第一搜索网络得到的；

[0030] 融合各所述第一网络输出得到第二网络输出，并根据所述第二网络输出和本端的标签数据计算损失函数相对于各所述第一网络输出的第一梯度；

[0031] 将各所述第一梯度进行差分隐私加密处理得到各第一加密梯度，将各所述第一加密梯度发送给对应的数据方，以供所述数据方根据所述第一加密梯度更新所述第一搜索网络中的搜索结构参数和/或模型参数。

[0032] 进一步地，所述接收所述数据方发送的第一网络输出，其中，所述第一网络输出是所述数据方将所述第一数据集输入所述第一搜索网络得到的的步骤包括：

[0033] 接收所述数据方发送的第一网络输出，其中，所述第一网络输出是所述数据方将所述第一数据集输入所述第一搜索网络进行处理得到网络原始输出，并对所述网络原始输出进行差分隐私加密处理后得到的。

[0034] 进一步地，所述标签方部署有输出网络以及基于所述标签方的数据特征构建的第二数据集和第二搜索网络，

[0035] 所述融合各所述第一网络输出得到第二网络输出的步骤包括：

[0036] 将所述第二数据集输入所述第二搜索网络得到第三网络输出；

[0037] 将所述第三网络输出和各所述第一网络输出进行拼接后输入所述输出网络得到第二网络输出；

[0038] 所述根据所述第二网络输出和本端的标签数据计算损失函数相对于各所述第一网络输出的第一梯度的步骤之后，处理器1001还可以用于调用存储器1005中存储的纵向联邦建模优化程序，并执行以下操作：

[0039] 根据所述第二网络输出和所述标签数据计算损失函数相对于所述第二搜索网络中目标参数的第二梯度，并根据所述第二梯度更新所述目标参数，其中，所述目标参数是所述第二搜索网络中的搜索结构参数和/或模型参数。

[0040] 进一步地，所述差分隐私加密处理包括裁剪处理和添加高斯噪声处理，所述将各所述第一梯度进行差分隐私加密处理得到各第一加密梯度的步骤包括：

[0041] 对所述第一梯度进行裁剪处理得到第一裁剪梯度，其中，所述第一裁剪梯度的二阶范数小于或等于第一预设阈值；

[0042] 生成服从目标高斯分布的噪声阵列，其中，所述目标高斯分布的均值为0，均方差为第二预设阈值，所述噪声阵列中各元素与所述第一梯度中各元素一一对应；

[0043] 采用所述噪声阵列对所述第一梯度进行添加高斯噪声处理得到第一加密梯度。

[0044] 进一步地，所述生成服从目标高斯分布的噪声阵列的步骤之前，还包括：

[0045] 获取本次纵向联邦建模的隐私级别和建模进度；

[0046] 根据所述隐私级别和所述建模进度设置所述第二预设阈值。

[0047] 当图1所示设备为参与纵向联邦建模的数据方时，在图1所示的设备中，用户接口1003主要用于与客户端进行数据通信；网络接口1004主要用于与参与纵向联邦建模的标签方建立通信连接，各数据方中分别部署有基于各自数据特征构建的第一数据集和第一搜索网络；处理器1001可以用于调用存储器1005中存储的纵向联邦建模优化程序，并执行以下操作：

[0048] 将所述第一数据集输入所述第一搜索网络得到网络原始输出；

[0049] 对所述网络原始输出进行差分隐私加密处理得到第一网络输出；

[0050] 将所述第一网络输出发送给参与纵向联邦建模的标签方，以供所述标签方对从各数据方接收到的所述第一网络输出进行融合得到第二网络输出后，根据所述第二网络输出和所述标签方的标签数据计算损失函数相对于各所述第一网络输出的第一梯度，并将所述第一梯度并返回给对应的数据方；

[0051] 根据从所述标签方接收到的所述第一梯度更新所述第一搜索网络中的搜索结构参数和/或模型参数。

[0052] 进一步地，数据方的所述第一搜索网络中搜索结构参数包括第一搜索网络中网络单元之间连接操作对应的权重，所述根据从所述标签方接收到的所述第一梯度更新所述第一搜索网络中的搜索结构参数和/或模型参数的步骤之后，处理器1001还可以用于调用存储器1005中存储的纵向联邦建模优化程序，并执行以下操作：

[0053] 根据更新参数后的第一搜索网络中的搜索结构参数从各连接操作中选取保留操

作；

[0054] 将各所述保留操作和各所述保留操作连接的网络单元所构成的模型作为目标模型。

[0055] 基于上述的结构，提出纵向联邦建模优化方法的各实施例。

[0056] 参照图2，图2为本申请纵向联邦建模优化方法第一实施例的流程示意图。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。本申请纵向联邦建模优化方法应用于参与纵向联邦学习的标签方，所述标签方与参与纵向联邦学习的各数据方通信连接，各数据方分别部署有基于各自数据特征构建的第一数据集和第一搜索网络，数据方和标签方可以是智能手机、个人计算机和服务器等设备。在本实施例中，纵向联邦建模优化方法包括：

[0057] 步骤S10，接收所述数据方发送的第一网络输出，其中，所述第一网络输出是所述数据方将所述第一数据集输入所述第一搜索网络得到的；

[0058] 在本实施例中，纵向联邦学习中的参与方分为两类，一类是拥有标签数据的标签方，一类是没有标签数据但拥有特征数据的数据方，一般情况下，标签方有一个，数据方有一个或多个。各个数据方可分别部署有基于各自数据特征构建的数据集和搜索网络；若标签方也拥有特征数据时，则标签方也可作为一个数据方，并部署基于其数据特征构建的数据集和搜索网络，既执行标签方的任务也执行数据方的任务。以下为避免指代不清，当将数据方和标签方单独描述时，将数据方的数据集和搜索网络称第一数据集和第一搜索网络，将标签方的数据集和搜索网络称第二数据集和第二搜索网络以示区分。各个参与方的数据集的样本维度是对齐的，也即，各个数据集的样本ID是相同的，但是各个参与方的数据特征可各不相同。各个参与方预先可采用加密样本对齐的方式来构建样本维度对齐的数据集，在此不进行详细赘述。搜索网络是指用于进行网络结构搜索（NAS）的网络，在本实施例中，各个参与方的搜索网络可以是各自预先根据DARTS（Differentiable Architecture Search，可微结构搜索）方法设计的网络。

[0059] 搜索网络中包括多个单元，每个单元对应一个网络层，其中部分单元之间设置

有连接操作，以其中两个单元为例，这两个单元之前的连接操作可以是预先设置的N种连接操作，并定义了每种连接操作对应的权重，该权重即搜索网络的搜索结构参数，单元内的网络层参数即搜索网络的模型参数。在模型训练过程中，需要进行网络结构搜索以优化更新搜索结构参数和模型参数，基于最终更新的搜索结构参数即可确定最终的网络结构，即确定保留哪个或哪些连接操作。由于该网络的结构是经过网络搜索之后才确定的，各个参与方不需要像设计传统纵向联邦学习的模型一样去设置模型的网络结构，从而降低了设计模型的难度。

[0060] 各个参与方的搜索网络组合构成一个任务模型，各搜索网络的网络输出经过融合后得到任务模型最终的输出。进一步地，任务模型还可包括用于对各个搜索网络的网络输出进行融合的输出网络，该输出网络被设置于连接在各个参与方的搜索网络之后，以各个搜索网络的输出数据作为输入数据，输出网络的输出结果即作为任务模型的最终输出。输出网络可部署于标签方，输出网络可以采用全连接层，或者其他复杂的神经网络结构，具体可根据模型预测任务不同而不同；输出网络的输出结果的形式也可根据具体模型预测任务设置，例如，当模型预测任务是图像分类时，输出网络的输出结果是输入图像所属的类别。

[0061] 各参与方需要联合一起优化更新任务模型，也即，联合更新各自搜索网络中的模型结构参数和模型参数，最终得到符合预测准确率要求的任务模型。具体地，在联合进行参数更新的过程中，数据方要更新各自搜索网络中的参数，则需要标签方中的标签数据来计算损失函数和梯度，标签方要计算损失函数和梯度，则需要数据方中的数据集和搜索网络。由于各参与方中的数据集以及标签方中的标签数据都可能是隐私数据，例如各个银行之间联合建模时，数据往往来源于办理银行相关业务的用户的数据，若数据方和标签方之间直接交互数据集中的数据、模型结构和模型参数，则各参与方之间会泄露数据隐私。因此，在本实施例中，数据方和标签方之间可交互用于更新各自搜索网络中模型参数和搜索结构参数的中间结果，并基于接收到的中间结果更新各自的搜索网络中模型参数和搜索结构参数，以对各自搜索网络进行更新，进而完成任务模型的更新。中间结果可以是参数的梯度，也可以是搜索网络的输出数据。具体地，当

参与方是数据方时，发送给标签方的中间结果可以是该端搜索网络的输出数据；当参与方是标签方时，发送给数据方的中间结果可以是计算得到的数据方所发送的输出数据对应的梯度。

[0062] 各个参与方可进行多轮联合更新参数。在一轮联合更新参数的过程中，数据方向标签方发送一次网络输出，标签方向数据方发送一次梯度，各参与方可以仅更新各自搜索网络中的模型结构参数，也可以仅更新各自搜索网络中的模型参数，也可以同时更新各自搜索网络中的模型结构参数和模型参数，也即，可更新模型结构参数和/或模型参数。经过多轮联合更新参数后，各参与方的搜索网络中的模型结构参数和模型参数均得到多次更新。具体地各轮联合更新参数时各参与方具体更新哪种参数可预先统一设置。

[0063] 具体地，在一轮联合更新参数的过程中，各个数据方将各自的第一数据集输入各自的第一搜索网络，经过第一搜索网络的处理得到输出结果，基于输出结果得到第一网络输出。各数据方将各自的第一网络输出发送给标签方。其中，数据方可将第一搜索网络的输出结果（也可称网络原始输出）直接作为第一网络输出，也可以将输出结果采用加密算法进行加密，将加密结果作为第一网络输出。例如采用同态加密方法进行加密或差分隐私加密方法进行加密。标签方接收各个数据方发送的第一网络输出。

[0064] 需要说明的是，参与方在各轮联合更新参数中可采用不同的数据集。具体地，参与方可将总的数据集划分为多个小的训练集（也可称为数据批），每轮采用一个小数据集参与联合更新参数，或者，参与方也可以是每轮联合参数更新前，从总的数据集中进行有放回的采样一批数据来参与该轮的联合参数更新。

[0065] 步骤S20，融合各所述第一网络输出得到第二网络输出，并根据所述第二网络输出和本端的标签数据计算损失函数相对于各所述第一网络输出的第一梯度；

[0066] 标签方融合各个第一网络输出得到第二网络输出。具体地，标签方可将各第一网络输出进行平均得到第二网络输出，或当标签方部署有输出网络时，可将各第一网络输出进行拼接后输入输出网络中，经过输出网络的处理得到第二网络输出。其中，拼接的方式可以是进行向量拼接。标签方根据第二网络输出和标签方的标签数据计算损失函数，该损失函数可以是回归问题的均方误差或分类

问题的交叉熵损失等，并计算损失函数相对于各个第一网络输出的第一梯度。根据损失函数计算梯度的方式可参照链式法则和梯度下降算法，在此不进行详细赘述。

[0067] 步骤S30，将各所述第一梯度进行差分隐私加密处理得到各第一加密梯度，将各所述第一加密梯度发送给对应的数据方，以供所述数据方根据所述第一加密梯度更新所述第一搜索网络中的搜索结构参数和/或模型参数。

[0068] 标签方在计算得到各个第一网络输出对应的第一梯度后，将第一梯度分别进行差分隐私加密处理得到各个第一加密梯度。其中，差分隐私（differential privacy）是密码学中的一种手段，旨在提供一种当从统计数据库查询时，最大化数据查询的准确性，同时最大限度减少识别其记录的机会，一种常见的差分隐私方法是在数据上添加随机化的噪音，本实施例中差分隐私加密处理方式可采用现有的差分隐私加密处理方式，在此不进行详细赘述。

[0069] 标签方将各个第一加密梯度发送给对应的数据方，也即，第一加密梯度对应的第一网络输出是由哪个数据方发送的，就将该第一加密梯度发送给哪个数据方。数据方在接收到第一加密梯度后，根据第一加密梯度更新其第一搜索网络中的搜索结构参数和/或模型参数。具体地，数据方根据链式法则和梯度下降算法，根据第一加密梯度计算得到损失函数相对于其搜索网络中搜索结构参数和/或模型参数的梯度，并根据梯度对应更新搜索结构参数和/或模型参数。也即分为三种情况，第一种：根据第一加密梯度计算得到损失函数相对于搜索结构参数的梯度，根据该梯度更新搜索结构参数；第二种：根据第一加密梯度计算损失函数相对于模型参数的梯度，根据该梯度更新模型参数；第三种：根据第一加密梯度计算损失函数相对于搜索结构参数的梯度，根据该梯度更新搜索结构参数，并根据第一加密梯度计算损失函数相对于模型参数的梯度，根据该梯度更新模型参数。至此完成一轮联合更新参数的过程。

[0070] 经过多轮联合更新参数后，参与方可根据其更新参数后的搜索网络得到目标模型。具体地，参与方的搜索网络中搜索结构参数可包括搜索网络中网络单元之间连接操作对应的权重。也即，网络单元之间设置了连接操作，每个连接操作对应一个权重。需要说明的是，并不是任意两个网络单元之间都设置有连接操

作。参与方可根据其更新后的搜索网络中的搜索结构参数，从各个连接操作中选取保留操作。具体地，对于每两个存在连接操作的网络单元，其之间有多条连接操作，可从多条连接操作中选出权重大的一个或多个连接操作作为保留操作。在确定保留操作后，将各保留操作以及各个保留操作连接的网络单元所构成的模型，作为参与方的目标模型。各个参与方可采用各自的目标模型联合完成具体的模型预测任务。

[0071] 在本实施例中，通过标签方接收数据方发送的第一网络输出，其中，第一网络输出是所述数据方将所述第一数据集输入所述第一搜索网络得到的；标签方融合各第一网络输出得到第二网络输出，并根据第二网络输出和本端的标签数据计算损失函数相对于各第一网络输出的第一梯度；将各第一梯度进行差分隐私加密处理得到各第一加密梯度，将各第一加密梯度发送给对应的数据方，以供数据方根据第一加密梯度更新第一搜索网络中的搜索结构参数和/或模型参数。在本申请中，由于标签方发送给数据方的梯度是经过差分隐私加密处理后的，数据方无法获知原始的梯度，从而避免了数据方根据梯度推导出标签方的标签数据和特征数据，也就避免了标签方中的隐私数据泄露给数据方，提升了在纵向联邦建模过程中标签方的数据安全性。并且，相比于现有纵向联邦学习中，各参与方需要人工花费大量人力物力预先设计模型结构的方式，本实施例实现了在纵向联邦建模过程中，各数据方只需要设置各自的搜索网络即可，搜索网络中各个网络单元之间的连接，也即模型结构，是在纵向联邦建模过程中通过优化更新搜索结构参数的方式自动确定的，实现了自动纵向联邦学习，不需要花费大量人力物力预先设置模型结构，降低了参与纵向联邦学习的门槛，使得纵向联邦学习能够被应用于更广泛的具体任务领域中去实现具体的任务，提高了纵向联邦学习的应用范围。且建模过程中，数据方向标签方发送的是搜索网络的输出，标签方向数据方发送的是差分隐私处理后的梯度，各个参与方之间并不会直接交互数据集和模型本身，从而一定程度上保障了各个参与方的数据安全和模型信息安全。

[0072] 进一步地，为进一步提升数据方的数据安全性，所述步骤S10可包括：

[0073] 步骤S101，接收所述数据方发送的第一网络输出，其中，所述第一网络输出是

所述数据方将所述第一数据集输入所述第一搜索网络进行处理得到网络原始输出，并对所述网络原始输出进行差分隐私加密处理后得到的。

[0074] 数据方可将其第一数据集输入其第一搜索网络进行处理得到网络原始输出，网络原始输出即第一搜索网络直接输出的结果。数据方将网络原始输出进行差分隐私加密处理得到第一网络输出，再将第一网络输出发送给标签方。也即，标签方接收到的各个数据方发送的第一网络输出是数据方进行差分隐私加密处理后的结果，而不是第一搜索网络的网络原始输出，标签方基于第一网络输出无法获知网络原始输出，从而避免了标签方根据网络原始输出推导出数据方的特征数据，也就进一步地避免了数据方中的隐私数据泄露给标签方，提升了数据方的数据安全性。

[0075] 进一步地，基于上述第一实施例，提出本申请纵向联邦建模优化方法第二实施例，在本实施例中，所述标签方部署有输出网络以及基于所述标签方的数据特征构建的第二数据集和第二搜索网络，所述步骤S20中融合各所述第一网络输出得到第二网络输出的步骤包括：

[0076] 步骤S201，将所述第二数据集输入所述第二搜索网络得到第三网络输出；

[0077] 在本实施例中，当标签方拥有特征数据时，标签方可部署基于标签方的数据特征构建的第二数据集和第二搜索网络。标签方还可部署有用于融合各个搜索网络的网络输出的输出网络。标签方在一轮联合更新参数过程中，可将第二数据集输入第二搜索网络，经过第二搜索网络的处理得到第三网络输出。

[0078] 步骤S202，将所述第三网络输出和各所述第一网络输出进行拼接后输入所述输出网络得到第二网络输出；

[0079] 标签方在融合各个第一网络输出时，将第三网络输出和各个第一网络输出进行拼接，也即，将各个网络输出进行拼接，将拼接结果输出网络，经过输出网络的处理得到第二网络输出。其中，各个网络输出可看做向量形式，对各个网络输出进行拼接可采用常用的向量拼接方式。

[0080] 所述步骤S20之后，还包括：

[0081] 步骤S40，根据所述第二网络输出和所述标签数据计算损失函数相对于所述第二搜索网络中目标参数的第二梯度，并根据所述第二梯度更新所述目标参数，

其中，所述目标参数是所述第二搜索网络中的搜索结构参数和/或模型参数。

[0082] 标签方在计算得到第二网络输出，根据第二网络输出和标签数据计算得到损失函数后，还可计算损失函数相对于第二搜索网络中目标参数的第二梯度，并根据第二梯度更新目标参数。其中，目标参数可以是第二搜索网络中的搜索结构参数和/或模型参数。也即分为三种情况，第一种：计算损失函数相对于搜索结构参数的梯度，根据该梯度更新搜索结构参数；第二种：计算损失函数相对于模型参数的梯度，根据该梯度更新模型参数；第三种：计算损失函数相对于搜索结构参数的梯度，根据该梯度更新搜索结构参数，并计算损失函数相对于模型参数的梯度，根据该梯度更新模型参数。

[0083] 进一步地，基于上述第一和/或二实施例，提出本申请纵向联邦建模优化方法第三实施例。在本实施例中，所述步骤S30中将各所述第一梯度进行差分隐私加密处理得到各第一加密梯度的步骤包括：

[0084] 步骤S301，对所述第一梯度进行裁剪处理得到第一裁剪梯度，其中，所述第一裁剪梯度的二阶范数小于或等于第一预设阈值；

[0085] 进一步地，在本实施例中，差分隐私加密处理可包括裁剪处理和添加高斯噪声处理两步。具体地，标签方对第一梯度进行裁剪处理得到第一裁剪梯度，经过裁剪后得到的第一裁剪梯度的二阶范数小于或等于第一预设阈值。其中，第一预设阈值是标签方预先设置的一个阈值。将第一梯度裁剪为二阶范数小于或等于第一预设阈值的第一裁剪梯度，目的是使得标签方各轮联合更新参数时计算得到的第一梯度的变化幅度较大时，第一裁剪梯度的变化被限制在一定范围内，从而使得数据方无法根据第一裁剪梯度来反推出标签方的原始数据。标签方可采用任意能够达到该目的的裁剪处理方式。

[0086] 进一步地，一种裁剪处理方式是，对于每一个第一梯度，标签方计算该第一梯度的二阶范数与第一预设阈值的比值，并从得到的比值和1中选取较大的值，采用该第一梯度除以该较大值，得到第一裁剪梯度。根据该方法计算得到的第一裁剪梯度的二阶范数是小于或等于第一预设阈值的。根据该方法，若i表示各数据方的标号，G_i表示各数据方对应的第一梯度，则第一裁剪梯度$G_i' = G_i / \max(1, ||Gi||_2 / D_A)$，其中，$D_A$表示标签方设置的第一预设阈值。需要说明

的是，根据标签方对待各个数据方的隐私级别不同，标签方可针对不同的数据方设置不同的第一预设阈值，隐私级别较高，则可设置较小的第一预设阈值，隐私级别较低，则可设置较大的第一预设阈值。

[0087] 步骤S302，生成服从目标高斯分布的噪声阵列，其中，所述目标高斯分布的均值为0，均方差为第二预设阈值，所述噪声阵列中各元素与所述第一梯度中各元素一一对应；

[0088] 步骤S303，采用所述噪声阵列对所述第一梯度进行添加高斯噪声处理得到第一加密梯度。

[0089] 标签方可生成服从目标高斯分布的噪声阵列，其中，目标高斯分布的均值为0，均方差为第二预设阈值，噪声阵列中各元素与第一梯度中各元素一一对应。其中，第二预设阈值可以是根据具体需要进行设置的，第二预设阈值可以是第一预设阈值的平方乘以一个系数的平方。第一梯度是矩阵形式，则生成的噪声阵列也是矩阵形式，并且噪声阵列的矩阵大小与第一梯度的矩阵大小相同。

[0090] 标签方采用噪声阵列对各个第一梯度进行添加高斯噪声处理得到各个第一加密梯度。具体地，对于每一个第一梯度，标签方将噪声阵列与第一梯度相加，也即，将第一梯度中各元素分别加上噪声阵列中对应位置的元素。由于第一加密梯度是经过裁剪处理和添加噪声处理后得到的结果，数据方无法根据第一加密梯度获知原始的第一梯度，从而无法推导出标签方的原始数据，从而提高了标签方的数据隐私。

[0091] 进一步地，所述方法还包括：

[0092] 步骤S50，获取本次纵向联邦建模的隐私级别和建模进度；

[0093] 步骤S60，根据所述隐私级别和所述建模进度设置所述第二预设阈值。

[0094] 标签方可在纵向联邦建模过程中设置第二预设阈值，也即，在各轮联合更新参数时，标签方可采用不同的第二预设阈值。具体地，标签方可获取本次纵向联邦建模的隐私级别和当前的建模进度。可以预先设置不同的隐私级别所对应的基准阈值，预先设置不同的建模进度对应的阈值变化幅度，其中，阈值变化幅度可以是负也可以是正，建模进度可以是损失函数的收敛速度、联合更新参数的轮次或时长。

[0095] 标签方获取到本次纵向联邦建模的隐私级别后，可根据映射级别确定对应的基准阈值，并根据当前的建模进度确定阈值变化幅度，将基准阈值加上阈值变化幅度，得到第二预设阈值。隐私级别与基准阈值之间的对应关系可以是级别越高基准阈值越大，级别越低基准阈值越小，从而使得隐私级别越高时添加的噪声越大，隐私级别较低时添加的噪声越小，灵活地根据隐私级别来设置噪声大小，避免了噪声过大导致数据失真，影响模型的预测准确率

[0096] 当建模进度是收敛速度时，收敛速度与阈值变化幅度之间的关系可以是收敛速度越快阈值变化幅度越大，收敛速度越慢阈值变化幅度越小，以使得当收敛速度比较慢，难以收敛时，能够通过较小的阈值变化幅度（可能为负），使得第二预设阈值减小，从而使得噪声减小，以促进损失函数的收敛，保证模型的预测准确率。当建模进度是联合更新参数的轮次时，轮次与阈值变化幅度之间的关系可以是轮次越大阈值变化幅度越小，轮次越小阈值变化幅度越大，以使得随着联合更新参数的轮次增多，损失函数趋近于收敛时，第二预设阈值越来越小，从而使得噪声逐渐减小，以促进损失函数的收敛，保证模型的预测准确率。当建模进度是联合更新参数的时长时，时长与阈值变化幅度之间的关系可以是时长越大阈值变化幅度越小，时长越小阈值变化幅度越大，以使得随着联合更新参数的时长越来越长，损失函数趋近于收敛时，第二预设阈值越来越小，从而使得噪声逐渐减小，以促进损失函数的收敛，保证模型的预测准确率。

[0097] 进一步地，如图3所示，为一种差分隐私加密通信信息的自动纵向联邦学习框架。A表示标签方，B表示数据方，i表示数据方的标号，N为数据方的个数。A拥有特征数据X_A和对应的标签数据Y_A，B_1、…、B_N分别拥有特征数据X_1、…、X_N。特征数据X_A、X_1、…、X_N有不同分布的数据特征。各参与方有一个搜索网络，即，Net_A、Net_1、…、Net_N，其对应的模型参数和搜索结构参数分别为W_A、W_1、…、W_N和α_A、α_1、…、α_N。A还部署有一个输出网络Net_{out}，用于计算Y_{out}。图中右下角的clip（x）表示对x进行裁剪处理，+N（0，σ^2）表示在裁剪处理结果上添加高斯噪声。

[0098] 进一步地，基于上述第一、第二和/或第三实施例，提出本申请纵向联邦建模优化方法第四实施例。在本实施例中，所述方法应用于参与纵向联邦建模的数

据方，各数据方中分别部署有基于各自数据特征构建的第一数据集和第一搜索网络，所述方法包括以下步骤：

[0099] 步骤A10，将所述第一数据集输入所述第一搜索网络得到网络原始输出；

[0100] 在本实施例中，纵向联邦学习中的参与方分为两类，一类是拥有标签数据的标签方，一类是没有标签数据但拥有特征数据的数据方，一般情况下，标签方有一个，数据方有一个或多个。各个数据方可分别部署有基于各自数据特征构建的数据集和搜索网络；若标签方也拥有特征数据时，则标签方也可作为一个数据方，并部署基于其数据特征构建的数据集和搜索网络，既执行标签方的任务也执行数据方的任务。以下为避免指代不清，当将数据方和标签方单独描述时，将数据方的数据集和搜索网络称第一数据集和第一搜索网络，将标签方的数据集和搜索网络称第二数据集和第二搜索网络以示区分。各个参与方的数据集的样本维度是对齐的，也即，各个数据集的样本ID是相同的，但是各个参与方的数据特征可各不相同。各个参与方预先可采用加密样本对齐的方式来构建样本维度对齐的数据集，在此不进行详细赘述。搜索网络是指用于进行网络结构搜索（NAS）的网络，在本实施例中，各个参与方的搜索网络可以是各自预先根据DARTS（Differentiable Architecture Search，可微结构搜索）方法设计的网络。

[0101] 搜索网络中包括多个单元，每个单元对应一个网络层，其中部分单元之间设置有连接操作，以其中两个单元为例，这两个单元之前的连接操作可以是预先设置的N种连接操作，并定义了每种连接操作对应的权重，该权重即搜索网络的搜索结构参数，单元内的网络层参数即搜索网络的模型参数。在模型训练过程中，需要进行网络结构搜索以优化更新搜索结构参数和模型参数，基于最终更新的搜索结构参数即可确定最终的网络结构，即确定保留哪个或哪些连接操作。由于该网络的结构是经过网络搜索之后才确定的，各个参与方不需要像设计传统纵向联邦学习的模型一样去设置模型的网络结构，从而降低了设计模型的难度。

[0102] 各个参与方的搜索网络组合构成一个任务模型，各搜索网络的网络输出经过融合后得到任务模型最终的输出。进一步地，任务模型还可包括用于对各个搜索

网络的网络输出进行融合的输出网络，该输出网络被设置于连接在各个参与方的搜索网络之后，以各个搜索网络的输出数据作为输入数据，输出网络的输出结果即作为任务模型的最终输出。输出网络可部署于标签方，输出网络可以采用全连接层，或者其他复杂的神经网络结构，具体可根据模型预测任务不同而不同；输出网络的输出结果的形式也可根据具体模型预测任务设置，例如，当模型预测任务是图像分类时，输出网络的输出结果是输入图像所属的类别。

[0103] 各参与方需要联合一起优化更新任务模型，也即，联合更新各自搜索网络中的模型结构参数和模型参数，最终得到符合预测准确率要求的任务模型。具体地，在联合进行参数更新的过程中，数据方要更新各自搜索网络中的参数，则需要标签方中的标签数据来计算损失函数和梯度，标签方要计算损失函数和梯度，则需要数据方中的数据集和搜索网络。由于各参与方中的数据集以及标签方中的标签数据都可能是隐私数据，例如各个银行之间联合建模时，数据往往来源于办理银行相关业务的用户的数据，若数据方和标签方之间直接交互数据集中的数据、模型结构和模型参数，则各参与方之间会泄露数据隐私。因此，在本实施例中，数据方和标签方之间可交互用于更新各自搜索网络中模型参数和搜索结构参数的中间结果，并基于接收到的中间结果更新各自的搜索网络中模型参数和搜索结构参数，以对各自搜索网络进行更新，进而完成任务模型的更新。中间结果可以是参数的梯度，也可以是搜索网络的输出数据。具体地，当参与方是数据方时，发送给标签方的中间结果可以是该端搜索网络的输出数据；当参与方是标签方时，发送给数据方的中间结果可以是计算得到的数据方所发送的输出数据对应的梯度。

[0104] 各个参与方可进行多轮联合更新参数。在一轮联合更新参数的过程中，数据方向标签方发送一次网络输出，标签方向数据方发送一次梯度，各参与方可以仅更新各自搜索网络中的模型结构参数，也可以仅更新各自搜索网络中的模型参数，也可以同时更新各自搜索网络中的模型结构参数和模型参数，也即，可更新模型结构参数和/或模型参数。经过多轮联合更新参数后，各参与方的搜索网络中的模型结构参数和模型参数均得到多次更新。具体地各轮联合更新参数时各参与方具体更新哪种参数可预先统一设置。

[0105] 具体地，在一轮联合更新参数的过程中，各个数据方将各自的第一数据集输入各自的第一搜索网络，经过第一搜索网络的处理得到输出结果，该输出结果为网络原始输出。

[0106] 需要说明的是，参与方在各轮联合更新参数中可采用不同的数据集。具体地，参与方可将总的数据集划分为多个小的训练集（也可称为数据批），每轮采用一个小数据集参与联合更新参数，或者，参与方也可以是每轮联合参数更新前，从总的数据集中进行有放回的采样一批数据来参与该轮的联合参数更新。

[0107] 步骤A20，对所述网络原始输出进行差分隐私加密处理得到第一网络输出；

[0108] 步骤A30，将所述第一网络输出发送给参与纵向联邦建模的标签方，以供所述标签方对从各数据方接收到的所述第一网络输出进行融合得到第二网络输出后，根据所述第二网络输出和所述标签方的标签数据计算损失函数相对于各所述第一网络输出的第一梯度，并将所述第一梯度并返回给对应的数据方；

[0109] 数据方对网络原始输出进行差分隐私加密处理得到第一网络输出，再将第一网络输出发送给标签方。本实施例中差分隐私加密处理方式可采用现有的差分隐私加密处理方式。也即，标签方接收到的各个数据方发送的第一网络输出是数据方进行差分隐私加密处理后的结果，而不是第一搜索网络的网络原始输出，标签方基于第一网络输出无法获知网络原始输出，从而避免了标签方根据网络原始输出推导出数据方的特征数据，也就进一步地避免了数据方中的隐私数据泄露给标签方，提升了数据方的数据安全性。

[0110] 进一步地，在一实施方式中，数据方对第一网络输出进行差分隐私处理的方式可参照上述第三实施例中标签方对第一梯度进行差分隐私处理的方式。根据该方法，若i表示各数据方的标号，O_i表示各数据方对应的第一网络输出，则对第一网络输出进行裁剪得到的结果$O_i' = O_i / \max(1, ||Oi||_2 / C_i)$，其中，Di表示数据方i设置的阈值。

[0111] 标签方接收各个数据方发送的第一网络输出，并融合各个第一网络输出得到第二网络输出。具体地，标签方可将各第一网络输出进行平均得到第二网络输出，或当标签方部署有输出网络时，可将各第一网络输出进行拼接后输入输出网络中，经过输出网络的处理得到第二网络输出。其中，拼接的方式可以是进行

向量拼接。标签方根据第二网络输出和标签方的标签数据计算损失函数，该损失函数可以是回归问题的均方误差或分类问题的交叉熵损失等，并计算损失函数相对于各个第一网络输出的第一梯度。根据损失函数计算梯度的方式可参照链式法则和梯度下降算法，在此不进行详细赘述。

[0112] 标签方在计算得到各个第一网络输出对应的第一梯度后，可将第一梯度发送给对应的数据方，也即，第一梯度对应的第一网络输出是由哪个数据方发送的，就将该第一梯度发送给哪个数据方。

[0113] 步骤A40，根据从所述标签方接收到的所述第一梯度更新所述第一搜索网络中的搜索结构参数和/或模型参数。

[0114] 数据方在接收到第一梯度后，根据第一梯度更新其第一搜索网络中的搜索结构参数和/或模型参数。具体地，数据方根据链式法则和梯度下降算法，根据第一梯度计算得到损失函数相对于其搜索网络中搜索结构参数和/或模型参数的梯度，并根据梯度对应更新搜索结构参数和/或模型参数。也即分为三种情况，第一种：根据第一梯度计算得到损失函数相对于搜索结构参数的梯度，根据该梯度更新搜索结构参数；第二种：根据第一梯度计算损失函数相对于模型参数的梯度，根据该梯度更新模型参数；第三种：根据第一梯度计算损失函数相对于搜索结构参数的梯度，根据该梯度更新搜索结构参数，并根据第一梯度计算损失函数相对于模型参数的梯度，根据该梯度更新模型参数。至此完成一轮联合更新参数的过程。

[0115] 经过多轮联合更新参数后，参与方可根据其更新参数后的搜索网络得到目标模型。各个参与方可采用各自的目标模型联合完成具体的模型预测任务。

[0116] 在本实施例中，通过数据方将第一数据集输入所述第一搜索网络得到网络原始输出，对网络原始输出进行差分隐私加密处理得到第一网络输出，将第一网络输出发送给标签方，以供标签方对从各数据方接收到的第一网络输出进行融合得到第二网络输出后，根据第二网络输出和标签方的标签数据计算损失函数相对于各第一网络输出的第一梯度，并将第一梯度并返回给对应的数据方；数据方根据从标签方接收到的第一梯度更新第一搜索网络中的搜索结构参数和/或模型参数。由于标签方发送给数据方的梯度是经过差分隐私加密处理后的，数据

方无法获知原始的梯度，从而避免了数据方根据梯度推导出标签方的标签数据和特征数据，也就进一步地避免了标签方中的隐私数据泄露给数据方，提升了标签方的数据安全性。并且，相比于现有纵向联邦学习中，各参与方需要人工花费大量人力物力预先设计模型结构的方式，本实施例实现了在纵向联邦建模过程中，各数据方只需要设置各自的搜索网络即可，搜索网络中各个网络单元之间的连接，也即模型结构，是在纵向联邦建模过程中通过优化更新搜索结构参数的方式自动确定的，实现了自动纵向联邦学习，不需要花费大量人力物力预先设置模型结构，降低了参与纵向联邦学习的门槛，使得纵向联邦学习能够被应用于更广泛的具体任务领域中去实现具体的任务，提高了纵向联邦学习的应用范围。且建模过程中，数据方向标签方发送的是搜索网络的输出，标签方向数据方发送的是差分隐私处理后的梯度，各个参与方之间并不会直接交互数据集和模型本身，从而一定程度上保障了各个参与方的数据安全和模型信息安全。

[0117] 进一步地，数据方的所述第一搜索网络中搜索结构参数包括第一搜索网络中网络单元之间连接操作对应的权重，所述步骤A40之后，还包括：

[0118] 步骤A50，根据更新参数后的第一搜索网络中的搜索结构参数从各连接操作中选取保留操作；

[0119] 步骤A60，将各所述保留操作和各所述保留操作连接的网络单元所构成的模型作为目标模型。

[0120] 数据方的搜索网络中搜索结构参数可包括搜索网络中网络单元之间连接操作对应的权重。也即，网络单元之间设置了连接操作，每个连接操作对应一个权重。需要说明的是，并不是任意两个网络单元之间都设置有连接操作。在经过多轮联合更新参数后，数据方可根据其更新后的搜索网络中的搜索结构参数，从各个连接操作中选取保留操作。具体地，对于每两个存在连接操作的网络单元，其之间有多条连接操作，可从多条连接操作中选出权重大的一个或多个连接操作作为保留操作。在确定保留操作后，将各保留操作以及各个保留操作连接的网络单元所构成的模型，作为参与方的目标模型。

[0121] 进一步地，在一实施方式中，各个参与方可以是部署于银行或其他金融机构的

设备，参与方中存储有各机构在业务处理过程中记录的用户数据。不同的机构涉及的具体业务存在差异，因此各个参与方的用户数据的特征可能不同，各个机构可基于各自的数据特征构建数据集，采用各自的数据集联合进行纵向联邦学习，通过扩充模型特征丰富度的方式来提升模型的预测性能。具体地，各个参与方可联合构建用户风险预测模型，用于在信贷业务、保险业务等等业务场景中预测用户的风险程度。各个参与方的数据特征可以根据实际经验选取与用户风险预测相关的风险特征，例如，用户的存款数额、用户的违约次数等等。

[0122] 各个参与方采用各自的数据集按照上述实施例中的方式联合进行纵向联邦建模，得到各自的目标模型。

[0123] 在得到各自的目标模型后，各参与方可联合对用户进行风险预测。数据方将目标用户其本端的第二风险特征对应的用户数据输入其本端的目标模型，经过目标模型的处理，得到第一模型输出。数据方将第一模型输出发送给数据应用提供方。标签方接收各个数据方发送的第一模型输出。

[0124] 标签方将目标用户在其本端的第一风险特征对应的用户数据输入其本端的目标模型，经过目标模型的处理，得到第二模型输出。标签方将各个第一模型输出和第二模型输出进行拼接，将拼接结果输入标签方本端的输出网络，经过输出网络的处理，输出得到目标用户的风险预测结果。

[0125] 进一步地，当目标用户的风险预测任务是数据方发起时，标签方可以将目标用户的风险预测结果发送给数据方，以供数据方根据目标用户的风险预测结果进行后续的业务处理，例如，根据风险预测结果确定是否对目标用户进行贷款。

[0126] 在本实施例中，各参与方只需要设置各自的搜索网络即可，不需要花费大量人力物力去设置精心设置模型结构，从而降低了参与纵向联邦学习的门槛，使得银行和其他金融机构能够更加方便地通过纵向联邦学习进行联合建模，进而通过联合建模得到的风险预测模型完成风险预测任务。并且，在纵向联邦建模和建模后采用模型进行风险预测的过程中，各个参与方不需要直接交互各自的数据集和模型本身，从而保障了各个参与方中的用户隐私数据的安全。并且，数据方将搜索网络的网络输出进行差分隐私加密处理后再发送给标签方，避免了标签方根据网络输出推导出数据方中的原始用户数据，从而进一步提升了数据

方的数据安全性。标签方将网络输出对应的梯度进行差分隐私加密处理后再发送给数据方，避免了数据方根据网络输出的梯度推导出标签方中的原始用户数据，从而进一步提升了标签方的数据安全性。

[0127] 此外本申请实施例还提出一种纵向联邦建模优化装置，所述装置部署于参与纵向联邦建模的标签方，所述标签方与参与纵向联邦建模的各数据方通信连接，各所述数据方中分别部署有基于各自数据特征构建的第一数据集和第一搜索网络，所述装置包括：

[0128] 接收模块，用于接收所述数据方发送的第一网络输出，其中，所述第一网络输出是所述数据方将所述第一数据集输入所述第一搜索网络得到的；

[0129] 计算模块，用于融合各所述第一网络输出得到第二网络输出，并根据所述第二网络输出和本端的标签数据计算损失函数相对于各所述第一网络输出的第一梯度；

[0130] 第一差分隐私处理模块，用于将各所述第一梯度进行差分隐私加密处理得到各第一加密梯度，将各所述第一加密梯度发送给对应的数据方，以供所述数据方根据所述第一加密梯度更新所述第一搜索网络中的搜索结构参数和/或模型参数。

[0131] 进一步地，所述接收模块还用于：

[0132] 接收所述数据方发送的第一网络输出，其中，所述第一网络输出是所述数据方将所述第一数据集输入所述第一搜索网络进行处理得到网络原始输出，并对所述网络原始输出进行差分隐私加密处理后得到的。

[0133] 进一步地，所述标签方部署有输出网络以及基于所述标签方的数据特征构建的第二数据集和第二搜索网络，所述计算模块包括：

[0134] 输入单元，用于将所述第二数据集输入所述第二搜索网络得到第三网络输出；

[0135] 拼接单元，用于将所述第三网络输出和各所述第一网络输出进行拼接后输入所述输出网络得到第二网络输出；

[0136] 所述装置还包括：

[0137] 第一更新模块，用于根据所述第二网络输出和所述标签数据计算损失函数相对于所述第二搜索网络中目标参数的第二梯度，并根据所述第二梯度更新所述目

标参数，其中，所述目标参数是所述第二搜索网络中的搜索结构参数和/或模型参数。

[0138] 进一步地，所述差分隐私加密处理包括裁剪处理和添加高斯噪声处理，所述第一差分隐私处理模块包括：

[0139] 裁剪处理单元，用于对所述第一梯度进行裁剪处理得到第一裁剪梯度，其中，所述第一裁剪梯度的二阶范数小于或等于第一预设阈值；

[0140] 生成单元，用于生成服从目标高斯分布的噪声阵列，其中，所述目标高斯分布的均值为0，均方差为第二预设阈值，所述噪声阵列中各元素与所述第一梯度中各元素一一对应；

[0141] 添加噪声单元，用于采用所述噪声阵列对所述第一梯度进行添加高斯噪声处理得到第一加密梯度。

[0142] 进一步地，所述装置还包括：

[0143] 获取模块，用于获取本次纵向联邦建模的隐私级别和建模进度；

[0144] 设置模块，用于根据所述隐私级别和所述建模进度设置所述第二预设阈值。

[0145] 此外本申请实施例还提出一种纵向联邦建模优化装置，所述装置部署于参与纵向联邦建模的数据方，各数据方中分别部署有基于各自数据特征构建的第一数据集和第一搜索网络，所述装置包括：

[0146] 输入模块，用于将所述第一数据集输入所述第一搜索网络得到网络原始输出；

[0147] 第二差分隐私处理模块，用于对所述网络原始输出进行差分隐私加密处理得到第一网络输出；

[0148] 发送模块，用于将所述第一网络输出发送给参与纵向联邦建模的标签方，以供所述标签方对从各数据方接收到的所述第一网络输出进行融合得到第二网络输出后，根据所述第二网络输出和所述标签方的标签数据计算损失函数相对于各所述第一网络输出的第一梯度，并将所述第一梯度并返回给对应的数据方；

[0149] 第二更新模块，用于根据从所述标签方接收到的所述第一梯度更新所述第一搜索网络中的搜索结构参数和/或模型参数。

[0150] 进一步地，数据方的所述第一搜索网络中搜索结构参数包括第一搜索网络中网络单元之间连接操作对应的权重，所述装置还包括：

[0151] 选取模块，用于根据更新参数后的第一搜索网络中的搜索结构参数从各连接操作中选取保留操作；

[0152] 确定模块，用于将各所述保留操作和各所述保留操作连接的网络单元所构成的模型作为目标模型。

[0153] 本申请纵向联邦建模优化装置的具体实施方式的拓展内容与上述纵向联邦建模优化方法各实施例基本相同，在此不做赘述。

[0154] 此外，本申请实施例还提出一种计算机可读存储介质，所述存储介质上存储有纵向联邦建模优化程序，所述纵向联邦建模优化程序被处理器执行时实现如下所述的纵向联邦建模优化方法的步骤。

[0155] 本申请纵向联邦建模优化设备和计算机可读存储介质的各实施例，均可参照本申请纵向联邦建模优化方法各实施例，此处不再赘述。

[0156] 上述本申请实施例序号仅仅为了描述，不代表实施例的优劣。

[0157] 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）执行本申请各实施例所述的方法。

[0158] 以上仅为本申请的优选实施例，并非因此限制本申请的专利范围，凡是利用本申请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，均同理包括在本申请的专利保护范围内。

权利要求书

[权利要求 1] 一种纵向联邦建模优化方法，其中，所述方法应用于参与纵向联邦建模的标签方，所述标签方与参与纵向联邦建模的各数据方通信连接，各所述数据方中分别部署有基于各自数据特征构建的第一数据集和第一搜索网络，所述方法包括以下步骤：

接收所述数据方发送的第一网络输出，其中，所述第一网络输出是所述数据方将所述第一数据集输入所述第一搜索网络得到的；

融合各所述第一网络输出得到第二网络输出，并根据所述第二网络输出和本端的标签数据计算损失函数相对于各所述第一网络输出的第一梯度；

将各所述第一梯度进行差分隐私加密处理得到各第一加密梯度，将各所述第一加密梯度发送给对应的数据方，以供所述数据方根据所述第一加密梯度更新所述第一搜索网络中的搜索结构参数和/或模型参数。

[权利要求 2] 如权利要求1所述的纵向联邦建模优化方法，其中，所述接收所述数据方发送的第一网络输出，其中，所述第一网络输出是所述数据方将所述第一数据集输入所述第一搜索网络得到的步骤包括：

接收所述数据方发送的第一网络输出，其中，所述第一网络输出是所述数据方将所述第一数据集输入所述第一搜索网络进行处理得到网络原始输出，并对所述网络原始输出进行差分隐私加密处理后得到的。

[权利要求 3] 如权利要求1所述的纵向联邦建模优化方法，其中，所述标签方部署有输出网络以及基于所述标签方的数据特征构建的第二数据集和第二搜索网络。

[权利要求 4] 如权利要求3所述的纵向联邦建模优化方法，其中，所述融合各所述第一网络输出得到第二网络输出的步骤包括：

将所述第二数据集输入所述第二搜索网络得到第三网络输出；

将所述第三网络输出和各所述第一网络输出进行拼接后输入所述输出网络得到第二网络输出；

所述根据所述第二网络输出和本端的标签数据计算损失函数相对于各所述第一网络输出的第一梯度的步骤之后，还包括：

根据所述第二网络输出和所述标签数据计算损失函数相对于所述第二搜索网络中目标参数的第二梯度，并根据所述第二梯度更新所述目标参数，其中，所述目标参数是所述第二搜索网络中的搜索结构参数和/或模型参数。

[权利要求 5] 如权利要求1至4任一项所述的纵向联邦建模优化方法，其中，所述差分隐私加密处理包括裁剪处理和添加高斯噪声处理，所述将各所述第一梯度进行差分隐私加密处理得到各第一加密梯度的步骤包括：

对所述第一梯度进行裁剪处理得到第一裁剪梯度，其中，所述第一裁剪梯度的二阶范数小于或等于第一预设阈值；

生成服从目标高斯分布的噪声阵列，其中，所述目标高斯分布的均值为0，均方差为第二预设阈值，所述噪声阵列中各元素与所述第一梯度中各元素一一对应；

采用所述噪声阵列对所述第一梯度进行添加高斯噪声处理得到第一加密梯度。

[权利要求 6] 如权利要求5所述的纵向联邦建模优化方法，其中，所述生成服从目标高斯分布的噪声阵列的步骤之前，还包括：

获取本次纵向联邦建模的隐私级别和建模进度；

根据所述隐私级别和所述建模进度设置所述第二预设阈值。

[权利要求 7] 如权利要求1所述的纵向联邦建模优化方法，其中，若标签方也拥有特征数据时，则标签方也作为一个数据方，并部署基于其数据特征构建的数据集和搜索网络，既执行标签方的任务也执行数据方的任务。

[权利要求 8] 如权利要求7所述的纵向联邦建模优化方法，其中，数据方的数据集和搜索网络为第一数据集和第一搜索网络，标签方的数据集和搜索网络为第二数据集和第二搜索网络。

[权利要求 9] 一种纵向联邦建模优化方法，其中，所述方法应用于参与纵向联邦建模的数据方，各数据方中分别部署有基于各自数据特征构建的第一数

据集和第一搜索网络，所述方法包括以下步骤：

将所述第一数据集输入所述第一搜索网络得到网络原始输出；

对所述网络原始输出进行差分隐私加密处理得到第一网络输出；

将所述第一网络输出发送给参与纵向联邦建模的标签方，以供所述标签方对从各数据方接收到的所述第一网络输出进行融合得到第二网络输出后，根据所述第二网络输出和所述标签方的标签数据计算损失函数相对于各所述第一网络输出的第一梯度，并将所述第一梯度并返回给对应的数据方；

根据从所述标签方接收到的所述第一梯度更新所述第一搜索网络中的搜索结构参数和/或模型参数。

[权利要求 10] 如权利要求9所述的纵向联邦建模优化方法，其中，数据方的所述第一搜索网络中搜索结构参数包括第一搜索网络中网络单元之间连接操作对应的权重，所述根据从所述标签方接收到的所述第一梯度更新所述第一搜索网络中的搜索结构参数和/或模型参数的步骤之后，还包括：

根据更新参数后的第一搜索网络中的搜索结构参数从各连接操作中选取保留操作；

将各所述保留操作和各所述保留操作连接的网络单元所构成的模型作为目标模型。

[权利要求 11] 一种纵向联邦建模优化设备，其中，所述纵向联邦建模优化设备包括：存储器、处理器及存储在所述存储器上并可在所述处理器上运行的纵向联邦建模优化程序，所述纵向联邦建模优化程序被所述处理器执行时实现以下步骤：

接收所述数据方发送的第一网络输出，其中，所述第一网络输出是所述数据方将所述第一数据集输入所述第一搜索网络得到的；

融合各所述第一网络输出得到第二网络输出，并根据所述第二网络输出和本端的标签数据计算损失函数相对于各所述第一网络输出的第一梯度；

将各所述第一梯度进行差分隐私加密处理得到各第一加密梯度，将各所述第一加密梯度发送给对应的数据方，以供所述数据方根据所述第一加密梯度更新所述第一搜索网络中的搜索结构参数和/或模型参数。

[权利要求 12] 如权利要求11所述的纵向联邦建模优化设备，其中，所述接收所述数据方发送的第一网络输出，其中，所述第一网络输出是所述数据方将所述第一数据集输入所述第一搜索网络得到的步骤包括：

接收所述数据方发送的第一网络输出，其中，所述第一网络输出是所述数据方将所述第一数据集输入所述第一搜索网络进行处理得到网络原始输出，并对所述网络原始输出进行差分隐私加密处理后得到的。

[权利要求 13] 如权利要求11所述的纵向联邦建模优化设备，其中，所述标签方部署有输出网络以及基于所述标签方的数据特征构建的第二数据集和第二搜索网络，

所述融合各所述第一网络输出得到第二网络输出的步骤包括：

将所述第二数据集输入所述第二搜索网络得到第三网络输出；

将所述第三网络输出和各所述第一网络输出进行拼接后输入所述输出网络得到第二网络输出；

所述根据所述第二网络输出和本端的标签数据计算损失函数相对于各所述第一网络输出的第一梯度的步骤之后，还包括：

根据所述第二网络输出和所述标签数据计算损失函数相对于所述第二搜索网络中目标参数的第二梯度，并根据所述第二梯度更新所述目标参数，其中，所述目标参数是所述第二搜索网络中的搜索结构参数和/或模型参数。

[权利要求 14] 如权利要求11至13中任一项所述的纵向联邦建模优化设备，其中，所述差分隐私加密处理包括裁剪处理和添加高斯噪声处理，所述将各所述第一梯度进行差分隐私加密处理得到各第一加密梯度的步骤包括：

对所述第一梯度进行裁剪处理得到第一裁剪梯度，其中，所述第一裁剪梯度的二阶范数小于或等于第一预设阈值；

生成服从目标高斯分布的噪声阵列，其中，所述目标高斯分布的均值为0，均方差为第二预设阈值，所述噪声阵列中各元素与所述第一梯度中各元素一一对应；

采用所述噪声阵列对所述第一梯度进行添加高斯噪声处理得到第一加密梯度。

[权利要求 15] 如权利要求14所述的纵向联邦建模优化方法，其中，所述生成服从目标高斯分布的噪声阵列的步骤之前，还包括：

获取本次纵向联邦建模的隐私级别和建模进度；

根据所述隐私级别和所述建模进度设置所述第二预设阈值。

[权利要求 16] 如权利要求11所述的纵向联邦建模优化方法，其中，若标签方也拥有特征数据时，则标签方也作为一个数据方，并部署基于其数据特征构建的数据集和搜索网络，既执行标签方的任务也执行数据方的任务。

[权利要求 17] 如权利要求16所述的纵向联邦建模优化方法，其中，数据方的数据集和搜索网络为第一数据集和第一搜索网络，标签方的数据集和搜索网络为第二数据集和第二搜索网络。

[权利要求 18] 一种纵向联邦建模优化设备，其中，所述纵向联邦建模优化设备包括：存储器、处理器及存储在所述存储器上并可在所述处理器上运行的纵向联邦建模优化程序，所述纵向联邦建模优化程序被所述处理器执行时实现以下步骤：

将所述第一数据集输入所述第一搜索网络得到网络原始输出；

对所述网络原始输出进行差分隐私加密处理得到第一网络输出；

将所述第一网络输出发送给参与纵向联邦建模的标签方，以供所述标签方对从各数据方接收到的所述第一网络输出进行融合得到第二网络输出后，根据所述第二网络输出和所述标签方的标签数据计算损失函数相对于各所述第一网络输出的第一梯度，并将所述第一梯度并返回给对应的数据方；

根据从所述标签方接收到的所述第一梯度更新所述第一搜索网络中的搜索结构参数和/或模型参数。

[权利要求 19] 如权利要求18所述的纵向联邦建模优化设备，其中，数据方的所述第一搜索网络中搜索结构参数包括第一搜索网络中网络单元之间连接操作对应的权重，所述根据从所述标签方接收到的所述第一梯度更新所述第一搜索网络中的搜索结构参数和/或模型参数的步骤之后，还包括：

根据更新参数后的第一搜索网络中的搜索结构参数从各连接操作中选取保留操作；

将各所述保留操作和各所述保留操作连接的网络单元所构成的模型作为目标模型。

[权利要求 20] 一种计算机可读存储介质，其中，所述计算机可读存储介质上存储有纵向联邦建模优化程序，所述纵向联邦建模优化程序被处理器执行时实现如权利要求1至10中任一项所述的纵向联邦建模优化方法的步骤。

WO 2022/016964 PCT/CN2021/093407

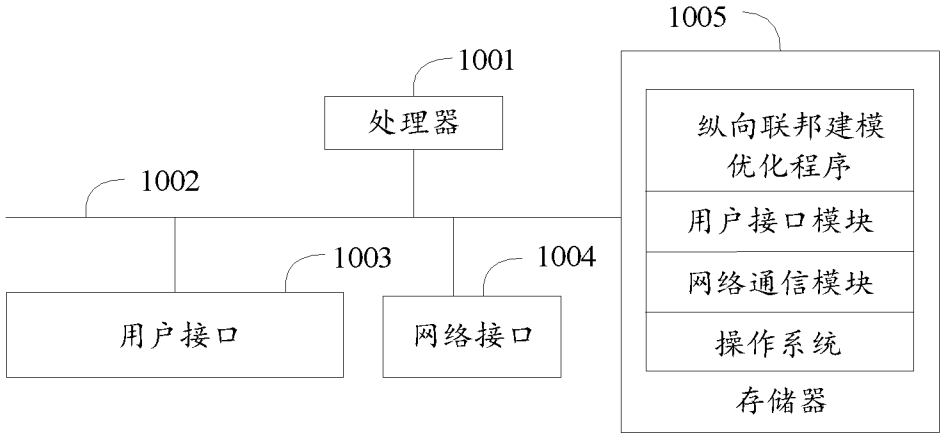

图 1

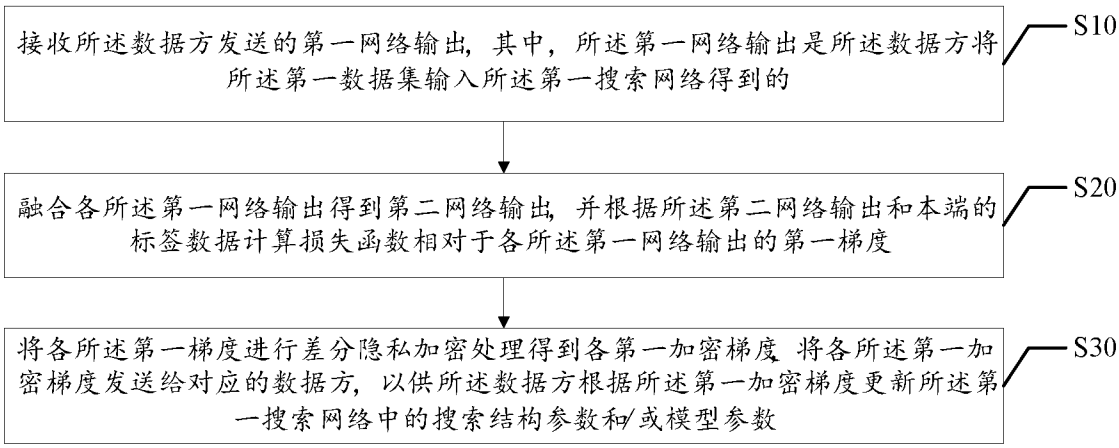

图 2

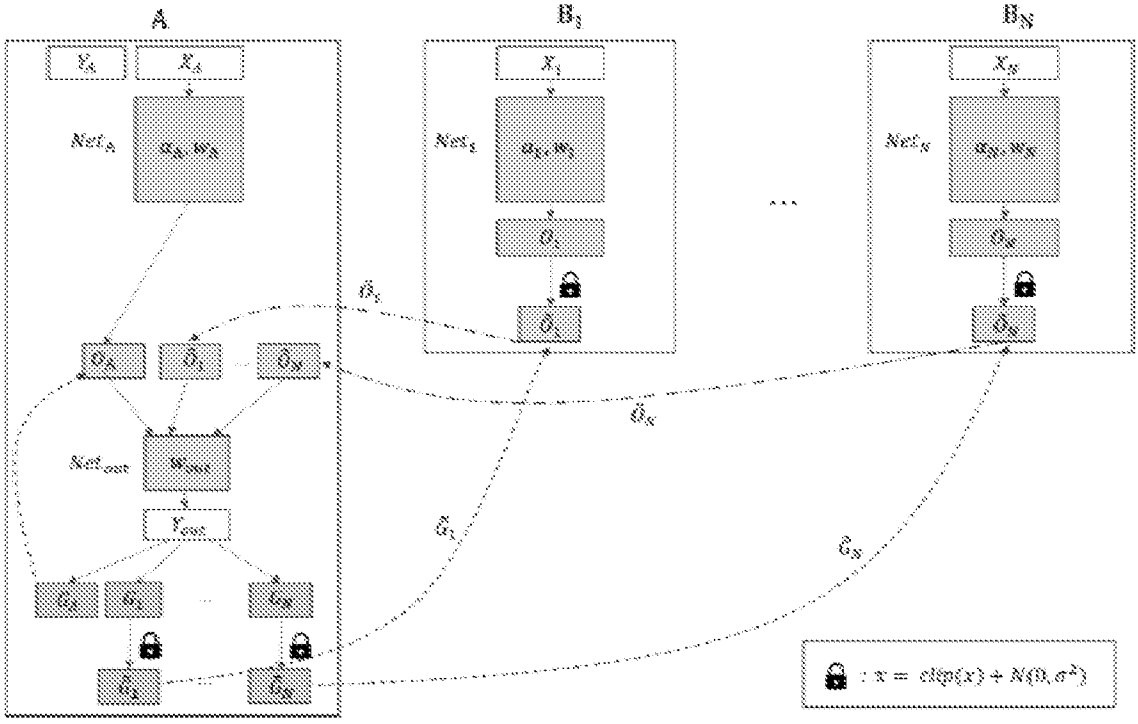

图 3

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2021/093407

A. CLASSIFICATION OF SUBJECT MATTER

G06N 20/00(2019.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06N

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNPAT, WPI, EPODOC, CNKI, IEEE: 联邦, 纵向, 标签, 搜索网络, 梯度, 更新, federa+, label, search , grads, update+, longitudinal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	CN 110633806 A (SHENZHEN QIANHAI WEBANK CO., LTD.) 31 December 2019 (2019-12-31) description, paragraphs 0048-0127, 182	1-20
Y	HE, Chaoyang et al. "FedNAS:Federated Deep Learning via Neural Architecture Search" *arXiv:2004.08546v1,* 18 April 2020 (2020-04-18), pp. 2-4	1-20
Y	CN 111210003 A (SHENZHEN QIANHAI WEBANK CO., LTD.) 29 May 2020 (2020-05-29) description paragraphs 0090-0111	3, 4, 13
A	CN 110633805 A (SHENZHEN QIANHAI WEBANK CO., LTD.) 31 December 2019 (2019-12-31) entire document	1-20
PX	CN 111860864 A (SHENZHEN QIANHAI WEBANK CO., LTD.) 30 October 2020 (2020-10-30) claims 1-10, description paragraphs 0118-0151	1-20

☐ Further documents are listed in the continuation of Box C. ☑ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
28 July 2021	**12 August 2021**
Name and mailing address of the ISA/CN **China National Intellectual Property Administration (ISA/CN)** **No. 6, Xitucheng Road, Jimenqiao, Haidian District, Beijing 100088** **China** Facsimile No. **(86-10)62019451**	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2021/093407

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 110633806 A	31 December 2019	None	
CN 111210003 A	29 May 2020	CN 111210003 B	19 March 2021
CN 110633805 A	31 December 2019	WO 2021004551 A1	14 January 2021
CN 111860864 A	30 October 2020	None	

国际检索报告

国际申请号
PCT/CN2021/093407

A. 主题的分类

G06N 20/00(2019.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

G06N

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用））

CNPAT, WPI, EPODOC, CNKI, IEEE: 联邦，纵向，标签，搜索网络，梯度，更新，federa+, label, search ,grads, update+, longitudinal

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
Y	CN 110633806 A (深圳前海微众银行股份有限公司) 2019年 12月 31日 (2019-12-31) 说明书第0048-0127，182段	1-20
Y	HE, Chaoyang 等. "FedNAS:Federated Deep Learning via Neural Architecture Search" arXiv:2004.08546v1, 2020年 4月 18日 (2020-04-18), 第2-4页	1-20
Y	CN 111210003 A (深圳前海微众银行股份有限公司) 2020年 5月 29日 (2020-05-29) 说明书第0090-0111段	3-4，13
A	CN 110633805 A (深圳前海微众银行股份有限公司) 2019年 12月 31日 (2019-12-31) 全文	1-20
PX	CN 111860864 A (深圳前海微众银行股份有限公司) 2020年 10月 30日 (2020-10-30) 权利要求1-10，说明书第0118-0151段	1-20

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2021年 7月 28日	2021年 8月 12日

ISA/CN的名称和邮寄地址	受权官员
中国国家知识产权局(ISA/CN) 中国 北京市海淀区蓟门桥西土城路6号 100088	胡丽丽
传真号 (86-10)62019451	电话号码 86-(10)-53961386

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2021/093407

检索报告引用的专利文件	公布日 (年/月/日)	同族专利	公布日 (年/月/日)
CN 110633806 A	2019年 12月 31日	无	
CN 111210003 A	2020年 5月 29日	CN 111210003 B	2021年 3月 19日
CN 110633805 A	2019年 12月 31日	WO 2021004551 A1	2021年 1月 14日
CN 111860864 A	2020年 10月 30日	无	