一种基于隐私保护的图模型训练方法、装置及设备

技术领域

[01]本说明书涉及计算机技术领域，尤其涉及一种基于隐私保护的图模型训练方法、装置及设备。

背景技术

[02]在大数据或人工智能应用场景中，许多任务需要利用用户数据来训练模型，而用户的个人隐私数据可能因为个人数据传输的过程遭到泄漏，因此，如何构建合理的隐私保护机器学习框架是当下最重要的话题之一。

[03]联邦学习是目前分布式学习中最重要的分支之一，联邦学习通过用户与服务器（数据使用方）交换模型梯度从而避免了直接传输用户的原始隐私数据，联邦学习相对于中心化的机器学习，实现了数据隔离从而保证了一定程度的用户隐私。随着图学习在工业界的大量应用和在学界的蓬勃发展，联邦图学习有着重要的应用前景，然而当前的联邦学习协议并不能保证用户的隐私安全，因为在某些特殊的机器学习模型下，可以通过截获传输的梯度信息直接破译用户的原始隐私数据。为此，需要提供一种能够更好保护用户隐私数据的联邦学习框架。

发明内容

[04]本说明书实施例的目的是提供一种能够更好保护用户隐私数据的联邦学习框架。

[05]为了实现上述技术方案，本说明书实施例是这样实现的：本说明书实施例提供的一种基于隐私保护的图模型训练方法，应用于终端设备，所述方法包括：获取待构建的第一图表的节点信息，以及第二图表的节点信息和节点连接信息。基于所述第一图表的节点信息，通过预设的全连接网络构建所述第一图表，并基于所述第二图表的节点信息和节点连接信息，通过预设的图网络构建所述第二图表，其中，所述全连接网络和所述图网络具有相同的网络参数。获取所述第一图表中存在训练标签信息的第一节点的隐向量，基于所述第一节点的隐向量和所述第一节点对应的训练标签信息，通过预设的 InstaHide 隐私保护规则构建第一样本数据。分别为所述第一图表中不存在训练标签信息的第二节点和所述第二图表中的节点生成相应的训练标签信息，获取所述第二节点和所述第二图表中的节点的隐向量，基于所述第二节点和所述第二图表中的节点的隐向量和生成的训练标签信息，通过预设的 InstaHide 隐私保护规则构建第二样本数据。基于所述第一样本数据和所述第二样本数据对服务器下发的图模型进行模型训练，并获取训练后的图模型对应的梯度信息，将所述梯度信息发送给所述服务器，以使所述服务器基于不同的终端设备提供的梯度信息对所述服务器中的图模型中的模型参数进行更新，得到更新后的图模型。

[06]本说明书实施例提供的一种基于隐私保护的图模型训练方法，应用于服务器，所述方法包括：接收多个不同的终端设备发送的图模型对应的梯度信息，所述图模型对应的梯度信息是所述终端设备基于获取的待构建的第一图表的节点信息，通过预设的全连接网络构建所述第一图表，并基于获取的第二图表的节点信息和节点连接信息，通过预设的图网络构建所述第二图表，基于所述第一图表中存在训练标签信息的第一节点的隐向量和所述第一节点对应的训练标签信息，通过预设的 InstaHide 隐私保护规则构建第一样本数据，并分别为所述第一图表中不存在训练标签信息的第二节点和所述第二图表中的节点生成相应的训练标签信息，基于所述第二节点和所述第二图表中的节点的隐向量和生成的训练标签信息，通过预设的 InstaHide 隐私保护规则构建第二样本数据，基于所述第一样本数据和所述第二样本数据对图模型进行模型训练后而得到的梯度信息。基于多个不同的终端设备发送的图模型对应的梯度信息，对所述图模型中的模型参数进行更新，得到更新后的图模型。将更新后的图模型发送给所述终端设备，以使所述终端设备基于更新后的图模型执行相应的业务处理。

[07]本说明书实施例提供的一种基于隐私保护的图模型训练方法，应用于区块链系统，

所述方法包括：基于预先部署于所述区块链系统中的智能合约向联邦学习框架中的多个不同的终端设备发送图模型的模型参数，所述智能合约用于触发联邦学习处理。基于所述智能合约，分别从所述多个不同的终端设备获取所述图模型对应的梯度信息，所述图模型对应的梯度信息是所述终端设备基于获取的待构建的第一图表的节点信息，通过预设的全连接网络构建所述第一图表，并基于获取的第二图表的节点信息和节点连接信息，通过预设的图网络构建所述第二图表，基于所述第一图表中存在训练标签信息的第一节点的隐向量和所述第一节点对应的训练标签信息，通过预设的 InstaHide 隐私保护规则构建第一样本数据，并分别为所述第一图表中不存在训练标签信息的第二节点和所述第二图表中的节点生成相应的训练标签信息，基于所述第二节点和所述第二图表中的节点的隐向量和生成的训练标签信息，通过预设的 InstaHide 隐私保护规则构建第二样本数据，基于所述第一样本数据和所述第二样本数据对图模型进行模型训练后而得到的梯度信息。基于多个不同的终端设备发送的图模型对应的梯度信息和所述智能合约，对所述图模型中的模型参数进行更新，得到更新后的图模型。将更新后的图模型提供给所述终端设备，以使所述终端设备基于更新后的图模型执行相应的业务处理。

[08]本说明书实施例提供的一种基于隐私保护的图模型训练装置，所述装置包括：信息获取模块，获取待构建的第一图表的节点信息，以及第二图表的节点信息和节点连接信息。图表构建模块，基于所述第一图表的节点信息，通过预设的全连接网络构建所述第一图表，并基于所述第二图表的节点信息和节点连接信息，通过预设的图网络构建所述第二图表，其中，所述全连接网络和所述图网络具有相同的网络参数。第一样本构建模块，获取所述第一图表中存在训练标签信息的第一节点的隐向量，基于所述第一节点的隐向量和所述第一节点对应的训练标签信息，通过预设的 InstaHide 隐私保护规则构建第一样本数据。第二样本构建模块，分别为所述第一图表中不存在训练标签信息的第二节点和所述第二图表中的节点生成相应的训练标签信息，获取所述第二节点和所述第二图表中的节点的隐向量，基于所述第二节点和所述第二图表中的节点的隐向量和生成的训练标签信息，通过预设的 InstaHide 隐私保护规则构建第二样本数据。梯度确定模块，基于所述第一样本数据和所述第二样本数据对服务器下发的图模型进行模型训练，并获取训练后的图模型对应的梯度信息，将所述梯度信息发送给所述服务器，以使所述服务器基于不同的终端设备提供的梯度信息对所述服务器中的图模型中的模型参数进行更新，得到更新后的图模型。

[09]本说明书实施例提供的一种基于隐私保护的图模型训练装置，所述装置包括：梯度接收模块，接收多个不同的终端设备发送的图模型对应的梯度信息，所述图模型对应的梯度信息是所述终端设备基于获取的待构建的第一图表的节点信息，通过预设的全连接网络构建所述第一图表，并基于获取的第二图表的节点信息和节点连接信息，通过预设的图网络构建所述第二图表，基于所述第一图表中存在训练标签信息的第一节点的隐向量和所述第一节点对应的训练标签信息，通过预设的 InstaHide 隐私保护规则构建第一样本数据，并分别为所述第一图表中不存在训练标签信息的第二节点和所述第二图表中的节点生成相应的训练标签信息，基于所述第二节点和所述第二图表中的节点的隐向量和生成的训练标签信息，通过预设的 InstaHide 隐私保护规则构建第二样本数据，基于所述第一样本数据和所述第二样本数据对图模型进行模型训练后而得到的梯度信息。模型参数更新模块，基于多个不同的终端设备发送的图模型对应的梯度信息，对所述图模型中的模型参数进行更新，得到更新后的图模型。发送模块，将更新后的图模型发送给所述终端设备，以使所述终端设备基于更新后的图模型执行相应的业务处理。

[10]本说明书实施例提供的一种基于隐私保护的图模型训练装置，所述装置为区块链系统中的装置，所述装置包括：模型参数下发模块，基于预先部署于所述区块链系统中的智能合约向联邦学习框架中的多个不同的终端设备发送图模型的模型参数，所述智能合约用于触发联邦学习处理。梯度获取模块，基于所述智能合约，分别从所述多个不同的

终端设备获取所述图模型对应的梯度信息，所述图模型对应的梯度信息是所述终端设备基于获取的待构建的第一图表的节点信息，通过预设的全连接网络构建所述第一图表，并基于获取的第二图表的节点信息和节点连接信息，通过预设的图网络构建所述第二图表，基于所述第一图表中存在训练标签信息的第一节点的隐向量和所述第一节点对应的训练标签信息，通过预设的 InstaHide 隐私保护规则构建第一样本数据，并分别为所述第一图表中不存在训练标签信息的第二节点和所述第二图表中的节点生成相应的训练标签信息，基于所述第二节点和所述第二图表中的节点的隐向量和生成的训练标签信息，通过预设的 InstaHide 隐私保护规则构建第二样本数据，基于所述第一样本数据和所述第二样本数据对图模型进行模型训练后而得到的梯度信息。模型参数更新模块，基于多个不同的终端设备发送的图模型对应的梯度信息和所述智能合约，对所述图模型中的模型参数进行更新，得到更新后的图模型。信息提供模块，将更新后的图模型提供给所述终端设备，以使所述终端设备基于更新后的图模型执行相应的业务处理。

[11]本说明书实施例提供的一种基于隐私保护的图模型训练设备，包括：处理器；以及被安排成存储计算机可执行指令的存储器，所述可执行指令在被执行时使所述处理器：获取待构建的第一图表的节点信息，以及第二图表的节点信息和节点连接信息。基于所述第一图表的节点信息，通过预设的全连接网络构建所述第一图表，并基于所述第二图表的节点信息和节点连接信息，通过预设的图网络构建所述第二图表，其中，所述全连接网络和所述图网络具有相同的网络参数。获取所述第一图表中存在训练标签信息的第一节点的隐向量，基于所述第一节点的隐向量和所述第一节点对应的训练标签信息，通过预设的 InstaHide 隐私保护规则构建第一样本数据。分别为所述第一图表中不存在训练标签信息的第二节点和所述第二图表中的节点生成相应的训练标签信息，获取所述第二节点和所述第二图表中的节点的隐向量，基于所述第二节点和所述第二图表中的节点的隐向量和生成的训练标签信息，通过预设的 InstaHide 隐私保护规则构建第二样本数据。基于所述第一样本数据和所述第二样本数据对服务器下发的图模型进行模型训练，并获取训练后的图模型对应的梯度信息，将所述梯度信息发送给所述服务器，以使所述服务器基于不同的终端设备提供的梯度信息对所述服务器中的图模型中的模型参数进行更新，得到更新后的图模型。

[12]本说明书实施例提供的一种基于隐私保护的图模型训练设备，包括：处理器；以及被安排成存储计算机可执行指令的存储器，所述可执行指令在被执行时使所述处理器：接收多个不同的终端设备发送的图模型对应的梯度信息，所述图模型对应的梯度信息是所述终端设备基于获取的待构建的第一图表的节点信息，通过预设的全连接网络构建所述第一图表，并基于获取的第二图表的节点信息和节点连接信息，通过预设的图网络构建所述第二图表，基于所述第一图表中存在训练标签信息的第一节点的隐向量和所述第一节点对应的训练标签信息，通过预设的 InstaHide 隐私保护规则构建第一样本数据，并分别为所述第一图表中不存在训练标签信息的第二节点和所述第二图表中的节点生成相应的训练标签信息，基于所述第二节点和所述第二图表中的节点的隐向量和生成的训练标签信息，通过预设的 InstaHide 隐私保护规则构建第二样本数据，基于所述第一样本数据和所述第二样本数据对图模型进行模型训练后而得到的梯度信息。基于多个不同的终端设备发送的图模型对应的梯度信息，对所述图模型中的模型参数进行更新，得到更新后的图模型。将更新后的图模型发送给所述终端设备，以使所述终端设备基于更新后的图模型执行相应的业务处理。

[13]本说明书实施例提供的一种基于隐私保护的图模型训练设备，所述设备为区块链系统中的设备，所述基于隐私保护的图模型训练设备包括：处理器；以及被安排成存储计算机可执行指令的存储器，所述可执行指令在被执行时使所述处理器：基于预先部署于所述区块链系统中的智能合约向联邦学习框架中的多个不同的终端设备发送图模型的模型参数，所述智能合约用于触发联邦学习处理。基于所述智能合约，分别从所述多个

不同的终端设备获取所述图模型对应的梯度信息，所述图模型对应的梯度信息是所述终端设备基于获取的待构建的第一图表的节点信息，通过预设的全连接网络构建所述第一图表，并基于获取的第二图表的节点信息和节点连接信息，通过预设的图网络构建所述第二图表，基于所述第一图表中存在训练标签信息的第一节点的隐向量和所述第一节点对应的训练标签信息，通过预设的 InstaHide 隐私保护规则构建第一样本数据，并分别为所述第一图表中不存在训练标签信息的第二节点和所述第二图表中的节点生成相应的训练标签信息，基于所述第二节点和所述第二图表中的节点的隐向量和生成的训练标签信息，通过预设的 InstaHide 隐私保护规则构建第二样本数据，基于所述第一样本数据和所述第二样本数据对图模型进行模型训练后而得到的梯度信息。基于多个不同的终端设备发送的图模型对应的梯度信息和所述智能合约，对所述图模型中的模型参数进行更新，得到更新后的图模型。将更新后的图模型提供给所述终端设备，以使所述终端设备基于更新后的图模型执行相应的业务处理。

[14]本说明书实施例还提供了一种存储介质，其中，所述存储介质用于存储计算机可执行指令，所述可执行指令在被执行时实现以下流程：获取待构建的第一图表的节点信息，以及第二图表的节点信息和节点连接信息。基于所述第一图表的节点信息，通过预设的全连接网络构建所述第一图表，并基于所述第二图表的节点信息和节点连接信息，通过预设的图网络构建所述第二图表，其中，所述全连接网络和所述图网络具有相同的网络参数。获取所述第一图表中存在训练标签信息的第一节点的隐向量，基于所述第一节点的隐向量和所述第一节点对应的训练标签信息，通过预设的 InstaHide 隐私保护规则构建第一样本数据。分别为所述第一图表中不存在训练标签信息的第二节点和所述第二图表中的节点生成相应的训练标签信息，获取所述第二节点和所述第二图表中的节点的隐向量，基于所述第二节点和所述第二图表中的节点的隐向量和生成的训练标签信息，通过预设的 InstaHide 隐私保护规则构建第二样本数据。基于所述第一样本数据和所述第二样本数据对服务器下发的图模型进行模型训练，并获取训练后的图模型对应的梯度信息，将所述梯度信息发送给所述服务器，以使所述服务器基于不同的终端设备提供的梯度信息对所述服务器中的图模型中的模型参数进行更新，得到更新后的图模型。

[15]本说明书实施例还提供了一种存储介质，其中，所述存储介质用于存储计算机可执行指令，所述可执行指令在被执行时实现以下流程：接收多个不同的终端设备发送的图模型对应的梯度信息，所述图模型对应的梯度信息是所述终端设备基于获取的待构建的第一图表的节点信息，通过预设的全连接网络构建所述第一图表，并基于获取的第二图表的节点信息和节点连接信息，通过预设的图网络构建所述第二图表，基于所述第一图表中存在训练标签信息的第一节点的隐向量和所述第一节点对应的训练标签信息，通过预设的 InstaHide 隐私保护规则构建第一样本数据，并分别为所述第一图表中不存在训练标签信息的第二节点和所述第二图表中的节点生成相应的训练标签信息，基于所述第二节点和所述第二图表中的节点的隐向量和生成的训练标签信息，通过预设的 InstaHide 隐私保护规则构建第二样本数据，基于所述第一样本数据和所述第二样本数据对图模型进行模型训练后而得到的梯度信息。基于多个不同的终端设备发送的图模型对应的梯度信息，对所述图模型中的模型参数进行更新，得到更新后的图模型。将更新后的图模型发送给所述终端设备，以使所述终端设备基于更新后的图模型执行相应的业务处理。

[16]本说明书实施例还提供了一种存储介质，其中，所述存储介质用于存储计算机可执行指令，所述可执行指令在被执行时实现以下流程：基于预先部署于区块链系统中的智能合约向联邦学习框架中的多个不同的终端设备发送图模型的模型参数，所述智能合约用于触发联邦学习处理。基于所述智能合约，分别从所述多个不同的终端设备获取所述图模型对应的梯度信息，所述图模型对应的梯度信息是所述终端设备基于获取的待构建的第一图表的节点信息，通过预设的全连接网络构建所述第一图表，并基于获取的第二图表的节点信息和节点连接信息，通过预设的图网络构建所述第二图表，基于所述第一

图表中存在训练标签信息的第一节点的隐向量和所述第一节点对应的训练标签信息，通过预设的 InstaHide 隐私保护规则构建第一样本数据，并分别为所述第一图表中不存在训练标签信息的第二节点和所述第二图表中的节点生成相应的训练标签信息，基于所述第二节点和所述第二图表中的节点的隐向量和生成的训练标签信息，通过预设的 InstaHide 隐私保护规则构建第二样本数据，基于所述第一样本数据和所述第二样本数据对图模型进行模型训练后而得到的梯度信息。基于多个不同的终端设备发送的图模型对应的梯度信息和所述智能合约，对所述图模型中的模型参数进行更新，得到更新后的图模型。将更新后的图模型提供给所述终端设备，以使所述终端设备基于更新后的图模型执行相应的业务处理。

附图说明

[17]图 1A 为本说明书一种基于隐私保护的图模型训练方法实施例；

[18]图 1B 为本说明书一种基于隐私保护的图模型训练的处理过程示意图；

[19]图 2 为本说明书一种基于隐私保护的图模型训练系统的结构示意图；

[20]图 3 为本说明书另一种基于隐私保护的图模型训练的处理过程示意图；

[21]图 4A 为本说明书另一种基于隐私保护的图模型训练方法实施例；

[22]图 4B 为本说明书又一种基于隐私保护的图模型训练的处理过程示意图；

[23]图 5A 为本说明书又一种基于隐私保护的图模型训练方法实施例；

[24]图 5B 为本说明书又一种基于隐私保护的图模型训练的处理过程示意图；

[25]图 6 为本说明书一种基于隐私保护的图模型训练装置实施例；

[26]图 7 为本说明书另一种基于隐私保护的图模型训练装置实施例；

[27]图 8 为本说明书又一种基于隐私保护的图模型训练装置实施例；

[28]图 9 为本说明书一种基于隐私保护的图模型训练设备实施例。

具体实施方式

[29]本说明书实施例提供一种基于隐私保护的图模型训练方法、装置及设备。

实施例一

[30]如图 1A 和图 1B 所示，本说明书实施例提供一种基于隐私保护的图模型训练方法，该方法的执行主体可以为终端设备，其中，该终端设备可以如手机、平板电脑、个人计算机等。该方法具体可以包括以下步骤：在步骤 S102 中，获取待构建的第一图表的节点信息，以及第二图表的节点信息和节点连接信息。

[31]其中，第一图表和第二图表可以是一种数据结构，第一图表和第二图表可以是图 Graph 等，本实施例中，第一图表和第二图表可以是属性图，属性图可以是由节点、边、标签、关系类型和属性组成的关系图，在属性图中，边也可以称为关系，节点和关系是最重要的实体，属性图的节点是独立存在的，可以为节点设置标签，拥有相同标签的节点属于同一个分组或同一个集合，关系可以通过关系类型进行分组，关系类型相同的关系属于同一个集合，关系可以是有向的，关系的两端是起始节点和结束节点，通过有向的箭头来标识方向，节点之间的双向关系通过两个方向相反的关系来标识，任意节点可以有 0 个、1 个或多个标签，但关系必须设置关系类型，并且只能设置一个关系类型。节点信息可以包括节点的标识(如节点 ID 或名称等)、节点的属性、节点的标签等信息，具体可以根据实际情况设定，本说明书实施例对此不做限定。节点连接信息可以是上述属性图中的关系，可以用于连接两个节点等，节点连接信息可以包括具有关联关系的两个节点的相关信息（如两个节点的标识等）和两个节点中哪个是起始节点，哪个是结束节点等，具体可以根据实际情况设定，本说明书实施例对此不做限定。

[32]在实施中，在大数据或人工智能应用场景中，许多任务需要利用用户数据来训练模型，而用户的个人隐私数据可能因为个人数据传输的过程遭到泄漏，因此，如何构建合理的隐私保护机器学习框架是当下最重要的话题之一。

[33]联邦学习是目前分布式学习中最重要的分支之一，联邦学习通过用户与服务器（数

据使用方）交换模型梯度从而避免了直接传输用户的原始隐私数据，联邦学习相对于中心化的机器学习，实现了数据隔离从而保证了一定程度的用户隐私。随着图学习在工业界的大量应用和在学界的蓬勃发展，联邦图学习有着重要的应用前景，然而当前的联邦学习协议并不能保证用户的隐私安全，因为在某些特殊的机器学习模型下，可以通过截获传输的梯度信息直接破译用户的原始隐私数据。为此，需要提供一种能够更好保护用户隐私数据的联邦学习框架。本说明书实施例提供一种可实现的联邦学习框架，具体可以包括以下内容:如图2所示,服务器可以根据预先设定的算法构建图模型的模型架构，该模型架构中可以包括待确定的模型参数，基于联邦学习机制，服务器构建图模型的模型架构后，可以将该图模型的模型架构发送给联邦学习的一个或多个不同的终端设备。在实际应用中，联邦学习的一个或多个不同的终端设备也可以根据服务器提供的相关信息（如使用的算法和图模型的相关信息等）构建图模型的模型架构，此时，服务器可以只需要将其构建的图模型的模型架构中模型参数发送给各个终端设备，终端设备接收到模型参数后，可以使用该模型参数对上述构建的图模型的模型架构中的模型参数进行更新，从而得到与服务器中的图模型的模型架构和模型参数均相同的图模型。在实际应用中，除了可以通过上述方式使得服务器与终端设备中最初的图模型相同外，还可以通过其它多种方式实现，具体可以根据实际情况设定，本说明书实施例对此不做限定。

[34]终端设备获取到图模型的模型架构后，可以从终端设备存储的数据中获取用于训练该图模型的数据，在实际应用中，终端设备可以对用户每次提供的数据进行存储，并可以将其作为用于训练该图模型的数据，此外，为了弥补终端设备自身存储的数据的不足，终端设备还可以采用指定的方式从其它设备中获取相应的数据，并可以将其作为用于训练该图模型的数据，具体可以根据实际情况设定。在终端设备获取的数据中可以包括具有完整图表信息的图表，也可以包括具有不完整图表信息的图表，为了后续说明方便，可以将具有完整图表信息的图表称为第二图表，第二图表可以包括一个，也可以包括多个，可以将具有不完整图表信息的图表称为第一图表，第一图表可以包括一个，也可以包括多个等，具体可以根据实际情况设定，本说明书实施例对此不做限定。本说明书实施例中，待构建的第一图表包括节点信息，不包括节点连接信息，第二图表包括节点信息和节点连接信息，基于此，终端设备可以获取待构建的第一图表的节点信息，以及第二图表的节点信息和节点连接信息。

[35]在步骤S104中，基于第一图表的节点信息，通过预设的全连接网络构建第一图表，并基于第二图表的节点信息和节点连接信息，通过预设的图网络构建第二图表，其中，全连接网络和图网络具有相同的网络参数。

[36]其中，全连接网络可以是相邻两个网络层之间任意两个节点之间存在连接关系的网络，全连接网络可以包括多个网络层，全连接网络中包含的网络层的数量可以根据实际设定，本说明书实施例对此不做限定。图网络可以是由节点，以及节点之间的连接关系构成的网络，图网络可以包括多种不同的架构，如知识图谱、递归神经网络等，具体可以根据实际情况设定，本说明书实施例对此不做限定。

[37]在实施中，由于第一图表不包含节点连接信息，为了构建第一图表，可以根据实际情况预先选取一个网络建立一个完整地第一图表，为了保证构建地第一图表不会遗漏信息，可以预先选取全连接网络，这样，可以使得相邻两个网络层之间任意两个节点之间均存在连接关系，具体地，可以根据第一图表的节点信息，并使用上述全连接网络将第一图表中的节点进行连接，得到第一图表。

[38]另外，由于第二图表中包含了完整的图表信息，因此，可以通过指定的图网络构建第二图表，其中，为了减少不同图网络构建的图表之间的差异或减少其它因素对最终结果的影响，可以设定上述全连接网络与该图网络具有相同的网络参数，即上述两个网络可以使用同一套网络参数（也即参数共享）。通过上述方式分别构建出第一图表和第二图表。

[39]在步骤 S106 中，获取第一图表中存在训练标签信息的第一节点的隐向量，基于第一节点的隐向量和第一节点对应的训练标签信息，通过预设的 InstaHide 隐私保护规则构建第一样本数据。

[40]其中，InstaHide 隐私保护规则可以是基于 Mixup 机制的隐私保护规则，即通过 Mixup 机制将样本数据与一个或多个随机样本数据混合，从而导致破译单个样本数据的难度显著加大，以此达到隐私保护的目的。Mixup 机制可以是一种样本数据的增强处理机制，具体地，针对原始的存在训练标签的样本数据，可以将每个样本数据对应的特征、训练标签与一个或多个其它样本数据计算平均值，得到 Mixup 机制处理的一个或多个样本数据。隐向量可以通过样本数据的表征来确定。

[41]在实施中，对于存在训练标签信息的数据（即第一图表中的第一节点对应的相关数据），可以先计算每个第一节点的表征，即得到第一图表中存在训练标签信息的第一节点的隐向量。基于第一节点的隐向量和第一节点对应的训练标签信息，可以构建新的数据集合，即由第一节点的隐向量和第一节点对应的训练标签信息构成的数据集合，可以将构建的新的数据集合转换为用于进行模型训练的样本数据。可以根据实际情况预先设定隐私保护规则，本实施例中可以通过 InstaHide 隐私保护规则实现，具体地，对于由第一节点的隐向量和第一节点对应的训练标签信息构成的数据集合，可以从上述第一节点的隐向量中随机选取一个隐向量，然后，可以从剩余的隐向量中选取一个或多个隐向量，可以计算上述选取的隐向量的平均值，得到相应的计算结果，通过相同的处理方式，对剩余的隐向量进行上述计算，分别得到每个隐向量对应的计算结果（为了后续描述方便，可以称为第一计算结果）。对于第一节点对应的训练标签信息，可以采用与上述隐向量相同的处理方式得到每个第一节点对应的训练标签信息对应的计算结果（为了后续描述方便，可以称为第二计算结果），可以基于第一计算结果和第二计算结果确定第一样本数据，例如，可以直接使用上述第一计算结果和第二计算结果构建第一样本数据，或者，可以分别对上述第一计算结果和第二计算结果进行指定的计算，分别得到相应的结算结果，可以基于上述得到的计算结果确定第一样本数据。

[42]在步骤 S108 中，分别为第一图表中不存在训练标签信息的第二节点和第二图表中的节点生成相应的训练标签信息，获取第二节点和第二图表中的节点的隐向量，基于第二节点和第二图表中的节点的隐向量和生成的训练标签信息，通过预设的 InstaHide 隐私保护规则构建第二样本数据。

[43]在实施中，由于第一图表和第二图表中还包括不存在训练标签信息的节点，因此，可以预先设定为上述节点设置训练标签信息的处理机制，例如，可以预先选取一种分类算法，可以通过该分类算法分别为上述节点进行分类，并通过相应的分类结果确定相应的训练标签信息，或者，可以预先训练一个机器学习模型（如神经网络模型等），通过训练的机器学习模型分别为第一图表中不存在训练标签信息的第二节点和第二图表中的节点确定相应的训练标签信息，此外，还可以通过其它多种不同的方式为第二节点和第二图表中的节点生成相应的训练标签信息，具体可以根据实际情况设定，本说明书实施例对此不做限定。

[44]通过上述方式得到不存在训练标签信息的节点对应的训练标签信息后，可以对上述节点执行如上述步骤 S106 的处理，从而构建第二样本数据，具体处理过程可以参见上述步骤 S106 的相关内容，在此不再赘述。

[45]在步骤 S110 中，基于第一样本数据和第二样本数据对服务器下发的图模型进行模型训练，并获取训练后的图模型对应的梯度信息，将该梯度信息发送给服务器，以使服务器基于不同的终端设备提供的梯度信息对服务器中的图模型中的模型参数进行更新，得到更新后的图模型。

[46]在实施中，通过上述方式得到终端设备中的样本数据后，可以使用该样本数据对服务器下发的图模型进行训练，直到图模型收敛，即可以得到训练后的图模型。然后，可

以计算训练后的图模型对应的梯度信息，可以将计算得到的梯度信息发送给服务器。服务器可以接收终端设备发送的梯度信息，此外，服务器也可以接收联邦学习中的其它终端设备提供的相应的终端设备训练后的图模型对应的梯度信息，服务器可以对接收到的梯度信息进行整合处理，并基于整合处理后的结果对服务器中的图模型的模型参数进行更新，得到最终的图模型，然后，可以将该图模型发送给联邦学习中的每个终端设备，终端设备可以使用更新后的图模型进行相应的业务处理，例如，终端设备可以使用更新后的图模型对某保险业务进行指定风险的防护与控制处理等。

[47]本说明书实施例提供一种基于隐私保护的图模型训练方法，基于第一图表的节点信息，通过预设的全连接网络构建第一图表，并基于第二图表的节点信息和节点连接信息，通过预设的图网络构建第二图表，其中，全连接网络和图网络具有相同的网络参数，然后，基于第一图表中存在训练标签信息的第一节点的隐向量和第一节点对应的训练标签信息，通过预设的 InstaHide 隐私保护规则构建第一样本数据，分别为第一图表中不存在训练标签信息的第二节点和第二图表中的节点生成相应的训练标签信息，并基于第二节点和第二图表中的节点的隐向量和生成的训练标签信息，通过预设的 InstaHide 隐私保护规则构建第二样本数据，最终可以基于第一样本数据和第二样本数据对服务器下发的图模型进行模型训练，并获取训练后的图模型对应的梯度信息，将该梯度信息发送给服务器，服务器基于不同的终端设备提供的梯度信息对服务器中的图模型中的模型参数进行更新，得到更新后的图模型，这样，基于 InstaHide 隐私保护规则可以提供合理的隐私保护水平并且具有较高的模型精度，使得从梯度信息破译用户的隐私数据难度急剧增加。

实施例二

[48]如图 3 所示，本说明书实施例提供一种基于隐私保护的图模型训练方法，该方法的执行主体可以为终端设备，其中，该终端设备可以如手机、平板电脑、个人计算机等。该方法具体可以包括以下步骤：

[49]在步骤 S302 中，获取待构建的第一图表的节点信息，以及第二图表的节点信息和节点连接信息。

[50]其中，第一图表和第二图表可以是属性图，如属性图 G=（V，E），表示一个节点集合 V 和边集合 E 的图，如果每个节点$v \in V$，允许有一个特征x_v，则图 G 即为属性图，可以记为 G=（V，E，X），其中，X 为每个节点的特征拼接而成的矩阵，在实际应用中，可以使用邻接矩阵 A 作为边集合的等价定义，A 是一个 N * N 的矩阵，N 为节点的个数，A{ij} = 1 表示节点 i 与节点 j 之间存在一条边，否则，A{ij} =0。

[51]在步骤 S304 中，基于第一图表的节点信息，通过预设的全连接网络构建第一图表，并基于第二图表的节点信息和节点连接信息，通过预设的图网络构建第二图表，其中，全连接网络和图网络具有相同的网络参数。

[52]其中，全连接网络可以为全卷积网络 FCN，上述图网络可以由图卷积神经网络 GCN、图注意力网络 GAT 或 GraphSAGE 构建。

[53]在步骤 S306 中，获取第一图表中存在训练标签信息的第一节点的隐向量。

[54]在步骤 S308 中，针对第一节点的隐向量和第一节点对应的训练标签信息，生成第一节点对应的置换函数和权重。

[55]其中，第一节点对应的权重的之和为 1。

[56]在实施中，可以采用 Mixup 机制确定第一节点对应的置换函数和权重，对于第一节点中的原始数据{$(x_1, y_1), (x_2, y_2), \ldots, (x_m, y_m)$}，其中 x 表示第一节点的特征，y 表示训练标签，通过 Mixup 机制可以将第一节点的特征进行转换，为此，可以预先设定置换函数π_i和相应的权重$\lambda_{i,\ k}$，其中，$1 \le i \le m$，且满足$\pi_i(i) = i$，则对于任意一个节点（即第 i 个节点），可以有

$$x_i' = \lambda_{i,1} \times x_{\pi_i(1)} + \lambda_{i,2} \times x_{\pi_i(2)} + \cdots + \lambda_{i,k} \times x_{\pi_i(k)} \qquad (1)$$

$$y_i' = \lambda_{i,1} \times y_{\pi_i(1)} + \lambda_{i,2} \times y_{\pi_i(2)} + \cdots + \lambda_{i,k} \times y_{\pi_i(k)} \quad (2)$$

$$\sum_j \lambda_{i,j} = 1 \quad (3)$$

[57]上述表达式所表达的含义可以为：对第 i 个样本，将其与 k−1 个随机选取的样本在样本数据的特征和训练标签信息上同时进行加权平均，然后，可以使用$\{(x_1', y_1'), (x_2', y_2'), \ldots, (x_m', y_m')\}$作为样本数据对相应的模型进行训练。

[58]同样的，对于第一图表中的第一节点，也可以使用与上述类似的方式得到相应的样本数据，对于第一图表中存在训练标签信息的第一节点，可以计算每个第一节点对应的特征，可以得到隐向量$f(x_i)$，其中，$1 \le i \le L$，则可以得到新的数据集合$\{(f(x_1), y_1), (f(x_2), y_2), \ldots, (f(x_L), y_L)\}$，其中，$f(x_i)$可以为 d 维向量。可以使用与上述公式（1）、公式（2）和公式（3）相同的方式得到：

$$f'_{(x_i)} = \lambda_{i,1} \times f(x_{\pi_i(1)}) + \lambda_{i,2} \times f(x_{\pi_i(2)}) + \cdots + \lambda_{i,k} \times f(x_{\pi_i(k)}) \quad (4)$$

$$y_i' = \lambda_{i,1} \times y_{\pi_i(1)} + \lambda_{i,2} \times y_{\pi_i(2)} + \cdots + \lambda_{i,k} \times y_{\pi_i(k)} \quad (5)$$

$$\sum_j \lambda_{i,j} = 1 \quad (6)$$

[59]求解上述表达式（4）、（5）和（6），最终可以得到第一节点对应的置换函数π_i和相应的权重$\lambda_{i,\ k}$。

[60]在步骤 S310 中，基于第一节点对应的置换函数和权重，以及第一节点的隐向量和第一节点对应的训练标签信息，生成第一预选样本数据。

[61]在实施中，可以基于上述公式（4）、公式（5）和公式（6），可以得到每个第一节点对应的置换函数和权重，然后，可以结合每个第一节点的隐向量和第一节点对应的训练标签信息最终可以得到

$$\{(f'_{(x_1)}, y_1'), (f'_{(x_2)}, y_2'), \ldots, (f'_{(x_L)}, y_L')\} \quad (7)$$

[62]上述表达式（7）即可以为第一预选样本数据。

[63]在步骤 S312 中，生成第一节点对应的节点参数，并基于第一节点对应的节点参数和第一预选样本数据，生成第一样本数据。

[64]其中，节点参数可以是根据实际情况设定，例如，节点参数可以是预先设定的指定向量，或者，也可以是随机向量等，具体可以根据实际情况设定，本说明书实施例对此不做限定。本实施例中，节点参数可以为 Rademacher 随机向量。

[65]在实施中，对每一个$n \in \{1,2,\ldots,L\}$，生成 d 维 Rademacher 随机向量$\sigma = (\sigma_1, \sigma_2, \ldots, \sigma_d)$，然后与$f(x_i)$逐维相乘，得到最终的第一样本数据。

[66]在步骤 S314 中，分别将第一图表中不存在训练标签信息的第二节点的节点数据和第二图表中的节点的节点数据输入到预设的目标图神经网络 GNN 模型中，分别得到与第一图表中不存在训练标签信息的第二节点和第二图表中的节点相应的训练标签信息，其中，目标 GNN 模型是基于预设的图表样本进行监督训练得到。

[67]在实施中，为了给没有训练标签信息的节点设置相应的训练标签信息，可以预先训练目标 GNN 模型，具体地，可以预先通过多种不同的方式（如购买或灰度测试等方式）获取用于训练上述目标 GNN 模型的样本数据（即图表样本，其中可以包括训练标签信息），然后，可以基于获取的图表样本对目标 GNN 模型进行监督训练，最终可以得到训练后的目标 GNN 模型。通过上述方式得到第一图表中不存在训练标签信息的第二节点的节点数据和第二图表中的节点的节点数据后，可以将上述获取的节点数据输入到训练后的目标 GNN 模型中，分别得到与第一图表中不存在训练标签信息的第二节点和第二图表中的节点相应的训练标签信息。

[68]在步骤 S316 中，获取第二节点和第二图表中的节点的隐向量，基于第二节点和第二图表中的节点的隐向量和生成的训练标签信息，通过预设的 InstaHide 隐私保护规则构建第二样本数据。

[69]在实施中，可以获取第二节点和第二图表中的节点的隐向量，针对第二节点和第二图表中的节点的隐向量和生成的训练标签信息，生成第二节点和第二图表中的节点对应

的置换函数和权重，基于第二节点和第二图表中的节点对应的置换函数和权重，以及生成的训练标签信息，生成第二预选样本数据，生成第二节点和第二图表中的节点对应的节点参数，并基于第二节点和第二图表中的节点对应的节点参数和第二预选样本数据，生成第二样本数据，上述过程的具体处理过程可以参见上述相关内容，在此不再赘述。

[70]在步骤 S318 中，基于第一样本数据对图模型进行模型训练，得到第一样本数据对应的预设第一分类损失函数的函数值。

[71]其中，图模型可以为基于图神经网络 GNN 构建。第一分类损失函数可以包括多种，具体可以根据实际情况选取，例如，第一分类损失函数可以为交叉熵损失函数等。

[72]在步骤 S320 中，基于第二样本数据对图模型进行模型训练，得到第二样本数据对应的预设第二分类损失函数的函数值。

[73]其中，第二分类损失函数可以包括多种，具体可以根据实际情况选取，例如，第二分类损失函数可以为交叉熵损失函数等。此外，第一分类损失函数和第二分类损失函数可以相同，即第一分类损失函数和第二分类损失函数为交叉熵损失函数等。

[74]在步骤 S322 中，基于第一样本数据对应的预设第一分类损失函数的函数值和第二样本数据对应的预设第二分类损失函数的函数值，确定图模型对应的损失函数的函数值，并基于图模型对应的损失函数的函数值，确定训练后的图模型对应的梯度信息，并将该梯度信息发送给服务器，以使服务器基于不同的终端设备提供的梯度信息对服务器中的图模型中的模型参数进行更新，得到更新后的图模型。

[75]在实施中，可以基于第一样本数据对应的预设第一分类损失函数的函数值和第二样本数据对应的预设第二分类损失函数的函数值，通过预设的整合规则对上述两部分损失进行整合，最终得到图模型对应的损失函数的函数值，然后，可以基于图模型对应的损失函数的函数值，并采用反向传播算法计算相应的梯度信息，得到训练后的图模型对应的梯度信息。

[76]需要说明的是，在部署推理时不需要部署全连接网络，仅需要部署图神经网络 GNN 进行常规推理即可。

[77]本说明书实施例提供一种基于隐私保护的图模型训练方法，基于第一图表的节点信息，通过预设的全连接网络构建第一图表，并基于第二图表的节点信息和节点连接信息，通过预设的图网络构建第二图表，其中，全连接网络和图网络具有相同的网络参数，然后，基于第一图表中存在训练标签信息的第一节点的隐向量和第一节点对应的训练标签信息，通过预设的 InstaHide 隐私保护规则构建第一样本数据，分别为第一图表中不存在训练标签信息的第二节点和第二图表中的节点生成相应的训练标签信息，并基于第二节点和第二图表中的节点的隐向量和生成的训练标签信息，通过预设的 InstaHide 隐私保护规则构建第二样本数据，最终可以基于第一样本数据和第二样本数据对服务器下发的图模型进行模型训练，并获取训练后的图模型对应的梯度信息，将该梯度信息发送给服务器，服务器基于不同的终端设备提供的梯度信息对服务器中的图模型中的模型参数进行更新，得到更新后的图模型，这样，基于 InstaHide 隐私保护规则可以提供合理的隐私保护水平并且具有较高的模型精度，使得从梯度信息破译用户的隐私数据难度急剧增加。

[78]此外，本说明书实施例设计了联邦学习协议下的图学习框架，并且具有隐私保护特性，本说明书实施例不仅提供了合理的隐私保护水平的同时避免了由于过量噪音等因素造成的模型精度损失，具有较好的适用性。

实施例三

[79]如图 4A 和图 4B 所示，本说明书实施例提供一种基于隐私保护的图模型训练方法，该方法的执行主体可以为服务器，其中，该服务器可以是为某项业务（如进行交易的业务或金融业务等）的服务器，具体如，该服务器可以是支付业务的服务器，也可以是与金融或即时通讯等相关业务的服务器等，或者，也可以是需要对业务数据进行风险检测

或基于隐私保护的图模型训练的服务器等。该方法具体可以包括以下步骤：在步骤 S402 中，接收多个不同的终端设备发送的图模型对应的梯度信息，图模型对应的梯度信息是终端设备基于获取的待构建的第一图表的节点信息，通过预设的全连接网络构建第一图表，并基于获取的第二图表的节点信息和节点连接信息，通过预设的图网络构建第二图表，基于第一图表中存在训练标签信息的第一节点的隐向量和第一节点对应的训练标签信息，通过预设的 InstaHide 隐私保护规则构建第一样本数据，并分别为第一图表中不存在训练标签信息的第二节点和第二图表中的节点生成相应的训练标签信息，基于第二节点和第二图表中的节点的隐向量和生成的训练标签信息，通过预设的 InstaHide 隐私保护规则构建第二样本数据，基于第一样本数据和第二样本数据对图模型进行模型训练后而得到的梯度信息。

[80]其中，图模型可以为基于图神经网络 GNN 构建。

[81]在步骤 S404 中，基于多个不同的终端设备发送的图模型对应的梯度信息，对图模型中的模型参数进行更新，得到更新后的图模型。

[82]上述步骤 S404 的具体处理可以包括多种，例如，可以对多个不同的终端设备发送的图模型对应的梯度信息进行整合处理，得到整合后的梯度信息，然后，可以基于整合后的梯度信息和图模型，可以计算得到模型参数的数值，然后可以使用计算得到的模型参数的数值对图模型中的模型参数进行更新，得到更新后的图模型。

[83]在实际应用中，上述步骤 S404 的具体处理，除了可以通过上述方式实现外，还可以通过多种不同的方式实现，以下再提供一种可选的处理方式，具体可以包括以下内容：基于多个不同的终端设备发送的图模型对应的梯度信息，通过预设的梯度更新策略对图模型中的模型参数进行更新，得到更新后的图模型，预设的梯度更新策略包括 FedAvg 梯度更新策略和 FedSgd 梯度更新策略中的一种或多种。

[84]其中，FedAvg 梯度更新策略可以是基于联邦平均的方式对梯度进行更新的策略，FedSgd 梯度更新策略可以是基于局部随机梯度下降（SGD）平均的方式对梯度进行更新的策略。

[85]在步骤 S406 中，将更新后的图模型发送给终端设备，以使终端设备基于更新后的图模型执行相应的业务处理。

[86]本说明书实施例提供一种基于隐私保护的图模型训练方法，基于第一图表的节点信息，通过预设的全连接网络构建第一图表，并基于第二图表的节点信息和节点连接信息，通过预设的图网络构建第二图表，其中，全连接网络和图网络具有相同的网络参数，然后，基于第一图表中存在训练标签信息的第一节点的隐向量和第一节点对应的训练标签信息，通过预设的 InstaHide 隐私保护规则构建第一样本数据，分别为第一图表中不存在训练标签信息的第二节点和第二图表中的节点生成相应的训练标签信息，并基于第二节点和第二图表中的节点的隐向量和生成的训练标签信息，通过预设的 InstaHide 隐私保护规则构建第二样本数据，最终可以基于第一样本数据和第二样本数据对服务器下发的图模型进行模型训练，并获取训练后的图模型对应的梯度信息，将该梯度信息发送给服务器，服务器基于不同的终端设备提供的梯度信息对服务器中的图模型中的模型参数进行更新，得到更新后的图模型，这样，基于 InstaHide 隐私保护规则可以提供合理的隐私保护水平并且具有较高的模型精度，使得从梯度信息破译用户的隐私数据难度急剧增加。

实施例四

[87]如图 5A 和图 5B 所示，本说明书实施例提供一种基于隐私保护的图模型训练方法，该方法的执行主体可以为区块链系统，该区块链系统可以由终端设备或服务器等组成，其中，终端设备可以如手机、平板电脑等移动终端设备，还可以如个人计算机等设备。该服务器可以是一个独立的服务器，还可以是由多个服务器构成的服务器集群等。该方法具体可以包括以下步骤：在步骤 S502 中，基于预先部署于区块链系统中的智能合约

向联邦学习框架中的多个不同的终端设备发送图模型的模型参数，该智能合约用于触发联邦学习处理。

[88]其中，智能合约中设置有用于触发联邦学习处理的规则，该规则可以包括一个，也可以包括多个。

[89]在实施中，可以预先基于联邦学习框架的处理过程构建智能合约，并可以将构建的智能合约部署于区块链系统中，以使得通过智能合约触发联邦学习处理。当需要进行联邦学习时，可以调用智能合约，通过智能合约中设定的相应规则触发为执行联邦学习的处理过程。

[90]需要说明的是，在实际应用中，图模型可以存储于区块链系统中，也可以存储于其它存储设备中，对于该图模型存储于其它存储设备中的情况，考虑到图模型可能需要进行定期或不定期更新，由于区块链系统具有不可篡改的特征，因此如果图模型存储于区块链系统中，后续需要对区块链系统中的图模型进行频繁的上传、删除和上传者的身份验证等操作，增大区块链系统的处理压力，为了提高处理效率，降低区块链系统的处理压力，可以预先将图模型存储于存储设备的指定存储地址内，而将该存储地址（即索引信息）上传于区块链系统中，由于该存储地址可以固定不变，并存储于区块链系统中，从而既保证了区块链系统中的数据的防篡改性，同时，图模型还可以在上述存储设备中进行定期或不定期的更新。

[91]基于上述内容，则上述步骤 S502 的处理还可以包括：基于预先部署于区块链系统中的智能合约获取联邦学习框架中的图模型的模型参数，基于该智能合约向联邦学习框架中的多个不同的终端设备发送该模型参数。

[92]在步骤 S504 中，基于上述智能合约，分别从多个不同的终端设备获取图模型对应的梯度信息，图模型对应的梯度信息是终端设备基于获取的待构建的第一图表的节点信息，通过预设的全连接网络构建第一图表，并基于获取的第二图表的节点信息和节点连接信息，通过预设的图网络构建第二图表，基于第一图表中存在训练标签信息的第一节点的隐向量和第一节点对应的训练标签信息，通过预设的 InstaHide 隐私保护规则构建第一样本数据，并分别为第一图表中不存在训练标签信息的第二节点和第二图表中的节点生成相应的训练标签信息，基于第二节点和第二图表中的节点的隐向量和生成的训练标签信息，通过预设的 InstaHide 隐私保护规则构建第二样本数据，基于第一样本数据和第二样本数据对图模型进行模型训练后而得到的梯度信息。

[93]在步骤 S506 中，基于多个不同的终端设备发送的图模型对应的梯度信息和上述智能合约，对图模型中的模型参数进行更新，得到更新后的图模型。

[94]基于上述内容，上述步骤 S506 的处理也可以通过下述方式处理：A2：基于上述智能合约，从区块链系统中获取该图模型的索引信息，并基于该索引信息获取该图模型。

[95]其中，索引信息可以用于记录图模型所存储的位置等信息，通过该索引信息，可以快速查找到相应的图模型，该索引信息相应的数据存储到区块链系统中后，通常不会对其内容进行修改，也即是该索引信息对应的图模型的存储位置通常不会改变，从而可以防止该索引信息被恶意篡改。

[96]在实施中，为了保证图模型的索引信息的完整性和防止被篡改，可以将图模型的索引信息上传至区块链系统中，具体地，为了记录图模型，可以根据实际情况预先设置该图模型的索引信息，如可以预先设置图模型能够存储的区域，然后，基于上述设置的区域生成索引信息等。在设置完成索引信息后，可以将该索引信息上传至区块链系统。

[97]A4：基于多个不同的终端设备发送的图模型对应的梯度信息和智能合约，对图模型中的模型参数进行更新，得到更新后的图模型。

[98]上述步骤 S506 的处理完成后，区块链系统还可以执行下述处理：基于上述索引信息和智能合约，将更新后的图模型存储于该索引信息对应的存储区域。

[99]另外，基于上述内容，上述步骤 S506 的处理还可以通过下述方式处理：B2：基于

上述智能合约，从区块链系统中获取上述图模型的索引信息。

[100]B4：基于上述智能合约触发上述索引信息对应存储组件基于多个不同的终端设备发送的图模型对应的梯度信息，对该图模型中的模型参数进行更新，得到更新后的图模型。

[101]此外，上述步骤 S506 的处理也可以通过下述方式处理：C2：基于上述智能合约，获取对该图模型中的模型参数进行更新的梯度更新策略，该梯度更新策略包括 FedAvg 梯度更新策略和 FedSgd 梯度更新策略中的一种或多种。

[102]C4：基于多个不同的终端设备发送的图模型对应的梯度信息，通过上述梯度更新策略对图模型中的模型参数进行更新，得到更新后的图模型。

[103]在步骤 S508 中，将更新后的图模型提供给终端设备，以使终端设备基于更新后的图模型执行相应的业务处理。

[104]基于上述 B2 和 B4 的处理方式，上述步骤 S508 的处理还可以通过下述方式实现：基于上述智能合约触发上述索引信息对应存储组件将更新后的图模型提供给终端设备。

[105]本说明书实施例提供一种基于隐私保护的图模型训练方法，基于预先部署于区块链系统中的智能合约向联邦学习框架中的多个不同的终端设备发送图模型的模型参数，基于智能合约，分别从多个不同的终端设备获取所述图模型对应的梯度信息，该图模型对应的梯度信息是终端设备基于获取的待构建的第一图表的节点信息，通过预设的全连接网络构建所述第一图表，并基于获取的第二图表的节点信息和节点连接信息，通过预设的图网络构建所述第二图表，基于第一图表中存在训练标签信息的第一节点的隐向量和所述第一节点对应的训练标签信息，通过预设的 InstaHide 隐私保护规则构建第一样本数据，并分别为第一图表中不存在训练标签信息的第二节点和第二图表中的节点生成相应的训练标签信息，基于第二节点和第二图表中的节点的隐向量和生成的训练标签信息，通过预设的 InstaHide 隐私保护规则构建第二样本数据，基于第一样本数据和第二样本数据对图模型进行模型训练后而得到的梯度信息，基于多个不同的终端设备发送的图模型对应的梯度信息和智能合约，对图模型中的模型参数进行更新，得到更新后的图模型，这样，基于 InstaHide 隐私保护规则可以提供合理的隐私保护水平并且具有较高的模型精度，使得从梯度信息破译用户的隐私数据难度急剧增加。

实施例五

[106]以上为本说明书实施例提供的基于隐私保护的图模型训练方法，基于同样的思路，本说明书实施例还提供一种基于隐私保护的图模型训练装置，如图 6 所示。

[107]该基于隐私保护的图模型训练装置包括：信息获取模块 601、图表构建模块 602、第一样本构建模块 603、第二样本构建模块 604 和梯度确定模块 605，其中：信息获取模块 601，获取待构建的第一图表的节点信息，以及第二图表的节点信息和节点连接信息；图表构建模块 602，基于所述第一图表的节点信息，通过预设的全连接网络构建所述第一图表，并基于所述第二图表的节点信息和节点连接信息，通过预设的图网络构建所述第二图表，其中，所述全连接网络和所述图网络具有相同的网络参数；第一样本构建模块 603，获取所述第一图表中存在训练标签信息的第一节点的隐向量，基于所述第一节点的隐向量和所述第一节点对应的训练标签信息，通过预设的 InstaHide 隐私保护规则构建第一样本数据；第二样本构建模块 604，分别为所述第一图表中不存在训练标签信息的第二节点和所述第二图表中的节点生成相应的训练标签信息，获取所述第二节点和所述第二图表中的节点的隐向量，基于所述第二节点和所述第二图表中的节点的隐向量和生成的训练标签信息，通过预设的 InstaHide 隐私保护规则构建第二样本数据；梯度确定模块 605，基于所述第一样本数据和所述第二样本数据对服务器下发的图模型进行模型训练，并获取训练后的图模型对应的梯度信息，将所述梯度信息发送给所述服务器，以使所述服务器基于不同的终端设备提供的梯度信息对所述服务器中的图模型中的模型参数进行更新，得到更新后的图模型。

[108]本说明书实施例中，所述全连接网络为全卷积网络 FCN，所述图网络由图卷积神经网络 GCN、图注意力网络 GAT 或 GraphSAGE 构建。

[109]本说明书实施例中，所述第一样本构建模块 603，包括：辅助参数生成单元，针对所述第一节点的隐向量和所述第一节点对应的训练标签信息，生成所述第一节点对应的置换函数和权重；预选样本生成单元，基于所述第一节点对应的置换函数和权重，以及所述第一节点的隐向量和所述第一节点对应的训练标签信息，生成第一预选样本数据；第一样本构建单元，生成所述第一节点对应的节点参数，并基于所述第一节点对应的节点参数和所述第一预选样本数据，生成所述第一样本数据。

[110]本说明书实施例中，所述第一节点对应的权重的和为 1。

[111]本说明书实施例中，所述梯度确定模块 605，包括：第一损失单元，基于所述第一样本数据对所述图模型进行模型训练，得到所述第一样本数据对应的预设第一分类损失函数的函数值；第二损失单元，基于所述第二样本数据对所述图模型进行模型训练，得到所述第二样本数据对应的预设第二分类损失函数的函数值；梯度确定单元，基于所述第一样本数据对应的预设第一分类损失函数的函数值和所述第二样本数据对应的预设第二分类损失函数的函数值，确定所述图模型对应的损失函数的函数值，并基于所述图模型对应的损失函数的函数值，确定训练后的图模型对应的梯度信息，并将所述梯度信息发送给服务器。

[112]本说明书实施例中，所述第一分类损失函数和所述第二分类损失函数相同，所述第一分类损失函数为交叉熵损失函数。

[113]本说明书实施例中，所述第二样本构建模块 604，分别将所述第一图表中不存在训练标签信息的第二节点的节点数据和所述第二图表中的节点的节点数据输入到预设的目标图神经网络 GNN 模型中，得到分别与所述第一图表中不存在训练标签信息的第二节点和所述第二图表中的节点相应的训练标签信息，其中，所述目标 GNN 模型是基于预设的图表样本进行监督训练得到。

[114]本说明书实施例中，所述图模型为基于图神经网络 GNN 构建。

[115]本说明书实施例提供一种基于隐私保护的图模型训练装置，基于第一图表的节点信息，通过预设的全连接网络构建第一图表，并基于第二图表的节点信息和节点连接信息，通过预设的图网络构建第二图表，其中，全连接网络和图网络具有相同的网络参数，然后，基于第一图表中存在训练标签信息的第一节点的隐向量和第一节点对应的训练标签信息，通过预设的 InstaHide 隐私保护规则构建第一样本数据，分别为第一图表中不存在训练标签信息的第二节点和所述第二图表中的节点生成相应的训练标签信息，并基于第二节点和第二图表中的节点的隐向量和生成的训练标签信息，通过预设的 InstaHide 隐私保护规则构建第二样本数据，最终可以基于第一样本数据和第二样本数据对服务器下发的图模型进行模型训练，并获取训练后的图模型对应的梯度信息，将该梯度信息发送给服务器，服务器基于不同的终端设备提供的梯度信息对服务器中的图模型中的模型参数进行更新，得到更新后的图模型，这样，基于 InstaHide 隐私保护规则可以提供合理的隐私保护水平并且具有较高的模型精度，使得从梯度信息破译用户的隐私数据难度急剧增加。

[116]此外，本说明书实施例设计了联邦学习协议下的图学习框架，并且具有隐私保护特性，本说明书实施例不仅提供了合理的隐私保护水平的同时避免了由于过量噪音等因素造成的模型精度损失，具有较好的适用性。

实施例六

[117]基于同样的思路，本说明书实施例还提供一种基于隐私保护的图模型训练装置，如图 7 所示。

[118]该基于隐私保护的图模型训练装置包括：梯度接收模块 701、模型参数更新模块 702 和发送模块 703，其中：梯度接收模块 701，接收多个不同的终端设备发送的图模型

对应的梯度信息，所述图模型对应的梯度信息是所述终端设备基于获取的待构建的第一图表的节点信息，通过预设的全连接网络构建所述第一图表，并基于获取的第二图表的节点信息和节点连接信息，通过预设的图网络构建所述第二图表，基于所述第一图表中存在训练标签信息的第一节点的隐向量和所述第一节点对应的训练标签信息，通过预设的 InstaHide 隐私保护规则构建第一样本数据，并分别为所述第一图表中不存在训练标签信息的第二节点和所述第二图表中的节点生成相应的训练标签信息，基于所述第二节点和所述第二图表中的节点的隐向量和生成的训练标签信息，通过预设的 InstaHide 隐私保护规则构建第二样本数据，基于所述第一样本数据和所述第二样本数据对图模型进行模型训练后而得到的梯度信息；模型参数更新模块 702，基于多个不同的终端设备发送的图模型对应的梯度信息，对所述图模型中的模型参数进行更新，得到更新后的图模型；发送模块 703，将更新后的图模型发送给所述终端设备，以使所述终端设备基于更新后的图模型执行相应的业务处理。

[119]本说明书实施例中，所述模型参数更新模块 702，基于多个不同的终端设备发送的图模型对应的梯度信息，通过预设的梯度更新策略对所述图模型中的模型参数进行更新，得到更新后的图模型，所述预设的梯度更新策略包括 FedAvg 梯度更新策略和 FedSgd 梯度更新策略中的一种或多种。

[120]本说明书实施例提供一种基于隐私保护的图模型训练装置，基于第一图表的节点信息，通过预设的全连接网络构建第一图表，并基于第二图表的节点信息和节点连接信息，通过预设的图网络构建第二图表，其中，全连接网络和图网络具有相同的网络参数，然后，基于第一图表中存在训练标签信息的第一节点的隐向量和第一节点对应的训练标签信息，通过预设的 InstaHide 隐私保护规则构建第一样本数据，分别为第一图表中不存在训练标签信息的第二节点和所述第二图表中的节点生成相应的训练标签信息，并基于第二节点和第二图表中的节点的隐向量和生成的训练标签信息，通过预设的 InstaHide 隐私保护规则构建第二样本数据，最终可以基于第一样本数据和第二样本数据对服务器下发的图模型进行模型训练，并获取训练后的图模型对应的梯度信息，将该梯度信息发送给服务器，服务器基于不同的终端设备提供的梯度信息对服务器中的图模型中的模型参数进行更新，得到更新后的图模型，这样，基于 InstaHide 隐私保护规则可以提供合理的隐私保护水平并且具有较高的模型精度，使得从梯度信息破译用户的隐私数据难度急剧增加。

实施例七

[121]基于同样的思路，本说明书实施例还提供一种基于隐私保护的图模型训练装置，所述装置为区块链系统中的装置，如图 8 所示。

[122]该基于隐私保护的图模型训练装置包括：模型参数下发模块 801、梯度获取模块 802、模型参数更新模块 803 和信息提供模块 804，其中：模型参数下发模块 801，基于预先部署于所述区块链系统中的智能合约向联邦学习框架中的多个不同的终端设备发送图模型的模型参数，所述智能合约用于触发联邦学习处理；梯度获取模块 802，基于所述智能合约，分别从所述多个不同的终端设备获取所述图模型对应的梯度信息，所述图模型对应的梯度信息是所述终端设备基于获取的待构建的第一图表的节点信息，通过预设的全连接网络构建所述第一图表，并基于获取的第二图表的节点信息和节点连接信息，通过预设的图网络构建所述第二图表，基于所述第一图表中存在训练标签信息的第一节点的隐向量和所述第一节点对应的训练标签信息，通过预设的 InstaHide 隐私保护规则构建第一样本数据，并分别为所述第一图表中不存在训练标签信息的第二节点和所述第二图表中的节点生成相应的训练标签信息，基于所述第二节点和所述第二图表中的节点的隐向量和生成的训练标签信息，通过预设的 InstaHide 隐私保护规则构建第二样本数据，基于所述第一样本数据和所述第二样本数据对图模型进行模型训练后而得到的梯度信息；模型参数更新模块 803，基于多个不同的终端设备发送的图模型对应的梯度

信息和所述智能合约，对所述图模型中的模型参数进行更新，得到更新后的图模型；信息提供模块 804，将更新后的图模型提供给所述终端设备，以使所述终端设备基于更新后的图模型执行相应的业务处理。

[123]本说明书实施例中，所述模型参数更新模块 803，包括：第一信息获取单元，基于所述智能合约，从所述区块链系统中获取所述图模型的索引信息，并基于所述索引信息获取所述图模型；第一模型参数更新单元，基于多个不同的终端设备发送的图模型对应的梯度信息和所述智能合约，对所述图模型中的模型参数进行更新，得到更新后的图模型；所述装置还包括：存储触发模块，基于所述索引信息和所述智能合约，将更新后的图模型存储于所述索引信息对应的存储区域。

[124]本说明书实施例中，所述模型参数更新模块 803，包括：第二信息获取单元，基于所述智能合约，从所述区块链系统中获取所述图模型的索引信息；第二模型参数更新单元，基于所述智能合约触发所述索引信息对应存储组件基于多个不同的终端设备发送的图模型对应的梯度信息，对所述图模型中的模型参数进行更新，得到更新后的图模型；所述信息提供模块，基于所述智能合约触发所述索引信息对应存储组件将更新后的图模型提供给所述终端设备。

[125]本说明书实施例提供一种基于隐私保护的图模型训练装置，基于预先部署于区块链系统中的智能合约向联邦学习框架中的多个不同的终端设备发送图模型的模型参数，基于智能合约，分别从多个不同的终端设备获取所述图模型对应的梯度信息，该图模型对应的梯度信息是终端设备基于获取的待构建的第一图表的节点信息，通过预设的全连接网络构建所述第一图表，并基于获取的第二图表的节点信息和节点连接信息，通过预设的图网络构建所述第二图表，基于第一图表中存在训练标签信息的第一节点的隐向量和所述第一节点对应的训练标签信息，通过预设的 InstaHide 隐私保护规则构建第一样本数据，并分别为第一图表中不存在训练标签信息的第二节点和第二图表中的节点生成相应的训练标签信息，基于第二节点和第二图表中的节点的隐向量和生成的训练标签信息，通过预设的 InstaHide 隐私保护规则构建第二样本数据，基于第一样本数据和第二样本数据对图模型进行模型训练后而得到的梯度信息，基于多个不同的终端设备发送的图模型对应的梯度信息和智能合约，对图模型中的模型参数进行更新，得到更新后的图模型，这样，基于 InstaHide 隐私保护规则可以提供合理的隐私保护水平并且具有较高的模型精度，使得从梯度信息破译用户的隐私数据难度急剧增加。

实施例八

[126]以上为本说明书实施例提供的基于隐私保护的图模型训练装置，基于同样的思路，本说明书实施例还提供一种基于隐私保护的图模型训练设备，如图 9 所示。

[127]所述基于隐私保护的图模型训练设备可以为上述实施例提供的服务器、终端设备或区块链系统的设备等。

[128]基于隐私保护的图模型训练设备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的处理器 901 和存储器 902，存储器 902 中可以存储有一个或一个以上存储应用程序或数据。其中，存储器 902 可以是短暂存储或持久存储。存储在存储器 902 的应用程序可以包括一个或一个以上模块（图示未示出），每个模块可以包括对基于隐私保护的图模型训练设备中的一系列计算机可执行指令。更进一步地，处理器 901 可以设置为与存储器 902 通信，在基于隐私保护的图模型训练设备上执行存储器 902 中的一系列计算机可执行指令。基于隐私保护的图模型训练设备还可以包括一个或一个以上电源 903，一个或一个以上有线或无线网络接口 904，一个或一个以上输入输出接口 905，一个或一个以上键盘 906。

[129]具体在本实施例中，基于隐私保护的图模型训练设备包括有存储器，以及一个或一个以上的程序，其中一个或者一个以上程序存储于存储器中，且一个或者一个以上程序可以包括一个或一个以上模块，且每个模块可以包括对基于隐私保护的图模型训练设

备中的一系列计算机可执行指令，且经配置以由一个或者一个以上处理器执行该一个或者一个以上程序包含用于进行以下计算机可执行指令：获取待构建的第一图表的节点信息，以及第二图表的节点信息和节点连接信息；基于所述第一图表的节点信息，通过预设的全连接网络构建所述第一图表，并基于所述第二图表的节点信息和节点连接信息，通过预设的图网络构建所述第二图表，其中，所述全连接网络和所述图网络具有相同的网络参数；获取所述第一图表中存在训练标签信息的第一节点的隐向量，基于所述第一节点的隐向量和所述第一节点对应的训练标签信息，通过预设的 InstaHide 隐私保护规则构建第一样本数据；分别为所述第一图表中不存在训练标签信息的第二节点和所述第二图表中的节点生成相应的训练标签信息，获取所述第二节点和所述第二图表中的节点的隐向量，基于所述第二节点和所述第二图表中的节点的隐向量和生成的训练标签信息，通过预设的 InstaHide 隐私保护规则构建第二样本数据；基于所述第一样本数据和所述第二样本数据对服务器下发的图模型进行模型训练，并获取训练后的图模型对应的梯度信息，将所述梯度信息发送给所述服务器，以使所述服务器基于不同的终端设备提供的梯度信息对所述服务器中的图模型中的模型参数进行更新，得到更新后的图模型。

[130]本说明书实施例中，所述全连接网络为全卷积网络 FCN，所述图网络由图卷积神经网络 GCN、图注意力网络 GAT 或 GraphSAGE 构建。

[131]本说明书实施例中，所述基于所述第一节点的隐向量和所述第一节点对应的训练标签信息，通过预设的 InstaHide 隐私保护规则构建第一样本数据，包括：针对所述第一节点的隐向量和所述第一节点对应的训练标签信息，生成所述第一节点对应的置换函数和权重；基于所述第一节点对应的置换函数和权重，以及所述第一节点的隐向量和所述第一节点对应的训练标签信息，生成第一预选样本数据；生成所述第一节点对应的节点参数，并基于所述第一节点对应的节点参数和所述第一预选样本数据，生成所述第一样本数据。

[132]本说明书实施例中，所述第一节点对应的权重的和为 1。

[133]本说明书实施例中，所述基于所述第一样本数据和所述第二样本数据对图模型进行模型训练，并获取训练后的图模型对应的梯度信息，将所述梯度信息发送给服务器，包括：基于所述第一样本数据对所述图模型进行模型训练，得到所述第一样本数据对应的预设第一分类损失函数的函数值；基于所述第二样本数据对所述图模型进行模型训练，得到所述第二样本数据对应的预设第二分类损失函数的函数值；基于所述第一样本数据对应的预设第一分类损失函数的函数值和所述第二样本数据对应的预设第二分类损失函数的函数值，确定所述图模型对应的损失函数的函数值，并基于所述图模型对应的损失函数的函数值，确定训练后的图模型对应的梯度信息，并将所述梯度信息发送给服务器。

[134]本说明书实施例中，所述第一分类损失函数和所述第二分类损失函数相同，所述第一分类损失函数为交叉熵损失函数。

[135]本说明书实施例中，所述分别为所述第一图表中不存在训练标签信息的第二节点和所述第二图表中的节点生成相应的训练标签信息，包括：分别将所述第一图表中不存在训练标签信息的第二节点的节点数据和所述第二图表中的节点的节点数据输入到预设的目标图神经网络 GNN 模型中，得到分别与所述第一图表中不存在训练标签信息的第二节点和所述第二图表中的节点相应的训练标签信息，其中，所述目标 GNN 模型是基于预设的图表样本进行监督训练得到。

[136]本说明书实施例中，所述图模型为基于图神经网络 GNN 构建。

[137]另外，具体在本实施例中，基于隐私保护的图模型训练设备包括有存储器，以及一个或一个以上的程序，其中一个或者一个以上程序存储于存储器中，且一个或者一个以上程序可以包括一个或一个以上模块，且每个模块可以包括对基于隐私保护的图模型训练设备中的一系列计算机可执行指令，且经配置以由一个或者一个以上处理器执行该

一个或者一个以上程序包含用于进行以下计算机可执行指令：接收多个不同的终端设备发送的图模型对应的梯度信息，所述图模型对应的梯度信息是所述终端设备基于获取的待构建的第一图表的节点信息，通过预设的全连接网络构建所述第一图表，并基于获取的第二图表的节点信息和节点连接信息，通过预设的图网络构建所述第二图表，基于所述第一图表中存在训练标签信息的第一节点的隐向量和所述第一节点对应的训练标签信息，通过预设的 InstaHide 隐私保护规则构建第一样本数据，并分别为所述第一图表中不存在训练标签信息的第二节点和所述第二图表中的节点生成相应的训练标签信息，基于所述第二节点和所述第二图表中的节点的隐向量和生成的训练标签信息，通过预设的 InstaHide 隐私保护规则构建第二样本数据，基于所述第一样本数据和所述第二样本数据对图模型进行模型训练后而得到的梯度信息；基于多个不同的终端设备发送的图模型对应的梯度信息，对所述图模型中的模型参数进行更新，得到更新后的图模型；将更新后的图模型发送给所述终端设备，以使所述终端设备基于更新后的图模型执行相应的业务处理。

[138]本说明书实施例中，所述基于多个不同的终端设备发送的图模型对应的梯度信息，对所述图模型中的模型参数进行更新，得到更新后的图模型，包括：基于多个不同的终端设备发送的图模型对应的梯度信息，通过预设的梯度更新策略对所述图模型中的模型参数进行更新，得到更新后的图模型，所述预设的梯度更新策略包括 FedAvg 梯度更新策略和 FedSgd 梯度更新策略中的一种或多种。

[139]另外，具体在本实施例中，基于隐私保护的图模型训练设备包括有存储器，以及一个或一个以上的程序，其中一个或者一个以上程序存储于存储器中，且一个或者一个以上程序可以包括一个或一个以上模块，且每个模块可以包括对基于隐私保护的图模型训练设备中的一系列计算机可执行指令，且经配置以由一个或者一个以上处理器执行该一个或者一个以上程序包含用于进行以下计算机可执行指令：基于预先部署于所述区块链系统中的智能合约向联邦学习框架中的多个不同的终端设备发送图模型的模型参数，所述智能合约用于触发联邦学习处理；基于所述智能合约，分别从所述多个不同的终端设备获取所述图模型对应的梯度信息，所述图模型对应的梯度信息是所述终端设备基于获取的待构建的第一图表的节点信息，通过预设的全连接网络构建所述第一图表，并基于获取的第二图表的节点信息和节点连接信息，通过预设的图网络构建所述第二图表，基于所述第一图表中存在训练标签信息的第一节点的隐向量和所述第一节点对应的训练标签信息，通过预设的 InstaHide 隐私保护规则构建第一样本数据，并分别为所述第一图表中不存在训练标签信息的第二节点和所述第二图表中的节点生成相应的训练标签信息，基于所述第二节点和所述第二图表中的节点的隐向量和生成的训练标签信息，通过预设的 InstaHide 隐私保护规则构建第二样本数据，基于所述第一样本数据和所述第二样本数据对图模型进行模型训练后而得到的梯度信息；基于多个不同的终端设备发送的图模型对应的梯度信息和所述智能合约，对所述图模型中的模型参数进行更新，得到更新后的图模型；将更新后的图模型提供给所述终端设备，以使所述终端设备基于更新后的图模型执行相应的业务处理。

[140]本说明书实施例中，所述基于多个不同的终端设备发送的图模型对应的梯度信息和所述智能合约，对所述图模型中的模型参数进行更新，得到更新后的图模型，包括：

[141]基于所述智能合约，从所述区块链系统中获取所述图模型的索引信息，并基于所述索引信息获取所述图模型；基于多个不同的终端设备发送的图模型对应的梯度信息和所述智能合约，对所述图模型中的模型参数进行更新，得到更新后的图模型；还包括：基于所述索引信息和所述智能合约，将更新后的图模型存储于所述索引信息对应的存储区域。

[142]本说明书实施例中，所述基于多个不同的终端设备发送的图模型对应的梯度信息和所述智能合约，对所述图模型中的模型参数进行更新，得到更新后的图模型，包括：

基于所述智能合约，从所述区块链系统中获取所述图模型的索引信息；基于所述智能合约触发所述索引信息对应存储组件基于多个不同的终端设备发送的图模型对应的梯度信息，对所述图模型中的模型参数进行更新，得到更新后的图模型；所述将更新后的图模型提供给所述终端设备，包括：基于所述智能合约触发所述索引信息对应存储组件将更新后的图模型提供给所述终端设备。

[143]本说明书实施例提供一种基于隐私保护的图模型训练设备，基于第一图表的节点信息，通过预设的全连接网络构建第一图表，并基于第二图表的节点信息和节点连接信息，通过预设的图网络构建第二图表，其中，全连接网络和图网络具有相同的网络参数，然后，基于第一图表中存在训练标签信息的第一节点的隐向量和第一节点对应的训练标签信息，通过预设的 InstaHide 隐私保护规则构建第一样本数据，分别为第一图表中不存在训练标签信息的第二节点和所述第二图表中的节点生成相应的训练标签信息，并基于第二节点和第二图表中的节点的隐向量和生成的训练标签信息，通过预设的 InstaHide 隐私保护规则构建第二样本数据，最终可以基于第一样本数据和第二样本数据对服务器下发的图模型进行模型训练，并获取训练后的图模型对应的梯度信息，将该梯度信息发送给服务器，服务器基于不同的终端设备提供的梯度信息对服务器中的图模型中的模型参数进行更新，得到更新后的图模型，这样，基于 InstaHide 隐私保护规则可以提供合理的隐私保护水平并且具有较高的模型精度，使得从梯度信息破译用户的隐私数据难度急剧增加。

[144]此外，本说明书实施例设计了联邦学习协议下的图学习框架，并且具有隐私保护特性，本说明书实施例不仅提供了合理的隐私保护水平的同时避免了由于过量噪音等因素造成的模型精度损失，具有较好的适用性。

实施例九

[145]进一步地，基于上述图 1A 和图 5B 所示的方法，本说明书一个或多个实施例还提供了一种存储介质，用于存储计算机可执行指令信息，一种具体的实施例中，该存储介质可以为 U 盘、光盘、硬盘等，该存储介质存储的计算机可执行指令信息在被处理器执行时，能实现以下流程：获取待构建的第一图表的节点信息，以及第二图表的节点信息和节点连接信息；基于所述第一图表的节点信息，通过预设的全连接网络构建所述第一图表，并基于所述第二图表的节点信息和节点连接信息，通过预设的图网络构建所述第二图表，其中，所述全连接网络和所述图网络具有相同的网络参数；获取所述第一图表中存在训练标签信息的第一节点的隐向量，基于所述第一节点的隐向量和所述第一节点对应的训练标签信息，通过预设的 InstaHide 隐私保护规则构建第一样本数据；分别为所述第一图表中不存在训练标签信息的第二节点和所述第二图表中的节点生成相应的训练标签信息，获取所述第二节点和所述第二图表中的节点的隐向量，基于所述第二节点和所述第二图表中的节点的隐向量和生成的训练标签信息，通过预设的 InstaHide 隐私保护规则构建第二样本数据；基于所述第一样本数据和所述第二样本数据对服务器下发的图模型进行模型训练，并获取训练后的图模型对应的梯度信息，将所述梯度信息发送给所述服务器，以使所述服务器基于不同的终端设备提供的梯度信息对所述服务器中的图模型中的模型参数进行更新，得到更新后的图模型。

[146]本说明书实施例中，所述全连接网络为全卷积网络 FCN，所述图网络由图卷积神经网络 GCN、图注意力网络 GAT 或 GraphSAGE 构建。

[147]本说明书实施例中，所述基于所述第一节点的隐向量和所述第一节点对应的训练标签信息，通过预设的 InstaHide 隐私保护规则构建第一样本数据，包括：针对所述第一节点的隐向量和所述第一节点对应的训练标签信息，生成所述第一节点对应的置换函数和权重；基于所述第一节点对应的置换函数和权重，以及所述第一节点的隐向量和所述第一节点对应的训练标签信息，生成第一预选样本数据；生成所述第一节点对应的节点参数，并基于所述第一节点对应的节点参数和所述第一预选样本数据，生成所述第一

样本数据。

[148]本说明书实施例中，所述第一节点对应的权重的和为 1。

[149]本说明书实施例中，所述基于所述第一样本数据和所述第二样本数据对图模型进行模型训练，并获取训练后的图模型对应的梯度信息，将所述梯度信息发送给服务器，包括：基于所述第一样本数据对所述图模型进行模型训练，得到所述第一样本数据对应的预设第一分类损失函数的函数值；基于所述第二样本数据对所述图模型进行模型训练，得到所述第二样本数据对应的预设第二分类损失函数的函数值；基于所述第一样本数据对应的预设第一分类损失函数的函数值和所述第二样本数据对应的预设第二分类损失函数的函数值，确定所述图模型对应的损失函数的函数值，并基于所述图模型对应的损失函数的函数值，确定训练后的图模型对应的梯度信息，并将所述梯度信息发送给服务器。

[150]本说明书实施例中，所述第一分类损失函数和所述第二分类损失函数相同，所述第一分类损失函数为交叉熵损失函数。

[151]本说明书实施例中，所述分别为所述第一图表中不存在训练标签信息的第二节点和所述第二图表中的节点生成相应的训练标签信息，包括：

[152]分别将所述第一图表中不存在训练标签信息的第二节点的节点数据和所述第二图表中的节点的节点数据输入到预设的目标图神经网络 GNN 模型中，得到分别与所述第一图表中不存在训练标签信息的第二节点和所述第二图表中的节点相应的训练标签信息，其中，所述目标 GNN 模型是基于预设的图表样本进行监督训练得到。

[153]本说明书实施例中，所述图模型为基于图神经网络 GNN 构建。

[154]在另一种具体的实施例中，该存储介质可以为 U 盘、光盘、硬盘等，该存储介质存储的计算机可执行指令信息在被处理器执行时，能实现以下流程：接收多个不同的终端设备发送的图模型对应的梯度信息，所述图模型对应的梯度信息是所述终端设备基于获取的待构建的第一图表的节点信息，通过预设的全连接网络构建所述第一图表，并基于获取的第二图表的节点信息和节点连接信息，通过预设的图网络构建所述第二图表，基于所述第一图表中存在训练标签信息的第一节点的隐向量和所述第一节点对应的训练标签信息，通过预设的 InstaHide 隐私保护规则构建第一样本数据，并分别为所述第一图表中不存在训练标签信息的第二节点和所述第二图表中的节点生成相应的训练标签信息，基于所述第二节点和所述第二图表中的节点的隐向量和生成的训练标签信息，通过预设的 InstaHide 隐私保护规则构建第二样本数据，基于所述第一样本数据和所述第二样本数据对图模型进行模型训练后而得到的梯度信息；基于多个不同的终端设备发送的图模型对应的梯度信息，对所述图模型中的模型参数进行更新，得到更新后的图模型；将更新后的图模型发送给所述终端设备，以使所述终端设备基于更新后的图模型执行相应的业务处理。

[155]本说明书实施例中，所述基于多个不同的终端设备发送的图模型对应的梯度信息，对所述图模型中的模型参数进行更新，得到更新后的图模型，包括：基于多个不同的终端设备发送的图模型对应的梯度信息，通过预设的梯度更新策略对所述图模型中的模型参数进行更新，得到更新后的图模型，所述预设的梯度更新策略包括 FedAvg 梯度更新策略和 FedSgd 梯度更新策略中的一种或多种。

[156]在另一种具体的实施例中，该存储介质可以为 U 盘、光盘、硬盘等，该存储介质存储的计算机可执行指令信息在被处理器执行时，能实现以下流程：基于预先部署于所述区块链系统中的智能合约向联邦学习框架中的多个不同的终端设备发送图模型的模型参数，所述智能合约用于触发联邦学习处理；基于所述智能合约，分别从所述多个不同的终端设备获取所述图模型对应的梯度信息，所述图模型对应的梯度信息是所述终端设备基于获取的待构建的第一图表的节点信息，通过预设的全连接网络构建所述第一图表，并基于获取的第二图表的节点信息和节点连接信息，通过预设的图网络构建所述第

二图表，基于所述第一图表中存在训练标签信息的第一节点的隐向量和所述第一节点对应的训练标签信息，通过预设的 InstaHide 隐私保护规则构建第一样本数据，并分别为所述第一图表中不存在训练标签信息的第二节点和所述第二图表中的节点生成相应的训练标签信息，基于所述第二节点和所述第二图表中的节点的隐向量和生成的训练标签信息，通过预设的 InstaHide 隐私保护规则构建第二样本数据，基于所述第一样本数据和所述第二样本数据对图模型进行模型训练后而得到的梯度信息；基于多个不同的终端设备发送的图模型对应的梯度信息和所述智能合约，对所述图模型中的模型参数进行更新，得到更新后的图模型；将更新后的图模型提供给所述终端设备，以使所述终端设备基于更新后的图模型执行相应的业务处理。

[157]本说明书实施例中，所述基于多个不同的终端设备发送的图模型对应的梯度信息和所述智能合约，对所述图模型中的模型参数进行更新，得到更新后的图模型，包括：基于所述智能合约，从所述区块链系统中获取所述图模型的索引信息，并基于所述索引信息获取所述图模型；基于多个不同的终端设备发送的图模型对应的梯度信息和所述智能合约，对所述图模型中的模型参数进行更新，得到更新后的图模型；还包括：基于所述索引信息和所述智能合约，将更新后的图模型存储于所述索引信息对应的存储区域。

[158]本说明书实施例中，所述基于多个不同的终端设备发送的图模型对应的梯度信息和所述智能合约，对所述图模型中的模型参数进行更新，得到更新后的图模型，包括：基于所述智能合约，从所述区块链系统中获取所述图模型的索引信息；基于所述智能合约触发所述索引信息对应存储组件基于多个不同的终端设备发送的图模型对应的梯度信息，对所述图模型中的模型参数进行更新，得到更新后的图模型；所述将更新后的图模型提供给所述终端设备，包括：基于所述智能合约触发所述索引信息对应存储组件将更新后的图模型提供给所述终端设备。

[159]本说明书实施例提供一种存储介质，基于第一图表的节点信息，通过预设的全连接网络构建第一图表，并基于第二图表的节点信息和节点连接信息，通过预设的图网络构建第二图表，其中，全连接网络和图网络具有相同的网络参数，然后，基于第一图表中存在训练标签信息的第一节点的隐向量和第一节点对应的训练标签信息，通过预设的 InstaHide 隐私保护规则构建第一样本数据，分别为第一图表中不存在训练标签信息的第二节点和所述第二图表中的节点生成相应的训练标签信息，并基于第二节点和第二图表中的节点的隐向量和生成的训练标签信息，通过预设的 InstaHide 隐私保护规则构建第二样本数据，最终可以基于第一样本数据和第二样本数据对服务器下发的图模型进行模型训练，并获取训练后的图模型对应的梯度信息，将该梯度信息发送给服务器，服务器基于不同的终端设备提供的梯度信息对服务器中的图模型中的模型参数进行更新，得到更新后的图模型，这样，基于 InstaHide 隐私保护规则可以提供合理的隐私保护水平并且具有较高的模型精度，使得从梯度信息破译用户的隐私数据难度急剧增加。

[160]此外，本说明书实施例设计了联邦学习协议下的图学习框架，并且具有隐私保护特性，本说明书实施例不仅提供了合理的隐私保护水平的同时避免了由于过量噪音等因素造成的模型精度损失，具有较好的适用性。

[161]上述对本说明书特定实施例进行了描述。其它实施例在所附权利要求书的范围内。在一些情况下，在权利要求书中记载的动作或步骤可以按照不同于实施例中的顺序来执行并且仍然可以实现期望的结果。另外，在附图中描绘的过程不一定要求示出的特定顺序或者连续顺序才能实现期望的结果。在某些实施方式中，多任务处理和并行处理也是可以的或者可能是有利的。

[162]在 20 世纪 90 年代，对于一个技术的改进可以很明显地区分是硬件上的改进（例如，对二极管、晶体管、开关等电路结构的改进）还是软件上的改进（对于方法流程的改进）。然而，随着技术的发展，当今的很多方法流程的改进已经可以视为硬件电路结构的直接改进。设计人员几乎都通过将改进的方法流程编程到硬件电路中来得到相应的

硬件电路结构。因此，不能说一个方法流程的改进就不能用硬件实体模块来实现。例如，可编程逻辑器件（Programmable Logic Device，PLD）（例如现场可编程门阵列（Field Programmable Gate Array，FPGA））就是这样一种集成电路，其逻辑功能由用户对器件编程来确定。由设计人员自行编程来把一个数字系统“集成”在一片 PLD 上，而不需要请芯片制造厂商来设计和制作专用的集成电路芯片。而且，如今，取代手工地制作集成电路芯片，这种编程也多半改用“逻辑编译器（logic compiler）”软件来实现，它与程序开发撰写时所用的软件编译器相类似，而要编译之前的原始代码也得用特定的编程语言来撰写，此称之为硬件描述语言（Hardware Description Language，HDL），而 HDL 也并非仅有一种，而是有许多种，如 ABEL（Advanced Boolean Expression Language）、AHDL（Altera Hardware Description Language）、Confluence、CUPL（Cornell University Programming Language）、HDCal、JHDL（Java Hardware Description Language）、Lava、Lola、MyHDL、PALASM、RHDL（Ruby Hardware Description Language）等，目前最普遍使用的是 VHDL（Very-High-Speed Integrated Circuit Hardware Description Language）与 Verilog。本领域技术人员也应该清楚，只需要将方法流程用上述几种硬件描述语言稍作逻辑编程并编程到集成电路中，就可以很容易得到实现该逻辑方法流程的硬件电路。

[163]控制器可以按任何适当的方式实现，例如，控制器可以采取例如微处理器或处理器以及存储可由该（微）处理器执行的计算机可读程序代码（例如软件或固件）的计算机可读介质、逻辑门、开关、专用集成电路（Application Specific Integrated Circuit，ASIC）、可编程逻辑控制器和嵌入微控制器的形式，控制器的例子包括但不限于以下微控制器：ARC 625D、Atmel AT91SAM、Microchip PIC18F26K20 以及 Silicone Labs C8051F320，存储器控制器还可以被实现为存储器的控制逻辑的一部分。本领域技术人员也知道，除了以纯计算机可读程序代码方式实现控制器以外，完全可以通过将方法步骤进行逻辑编程来使得控制器以逻辑门、开关、专用集成电路、可编程逻辑控制器和嵌入微控制器等的形式来实现相同功能。因此这种控制器可以被认为是一种硬件部件，而对其内包括的用于实现各种功能的装置也可以视为硬件部件内的结构。或者甚至，可以将用于实现各种功能的装置视为既可以是实现方法的软件模块又可以是硬件部件内的结构。

[164]上述实施例阐明的系统、装置、模块或单元，具体可以由计算机芯片或实体实现，或者由具有某种功能的产品来实现。一种典型的实现设备为计算机。具体的，计算机例如可以为个人计算机、膝上型计算机、蜂窝电话、相机电话、智能电话、个人数字助理、媒体播放器、导航设备、电子邮件设备、游戏控制台、平板计算机、可穿戴设备或者这些设备中的任何设备的组合。

[165]为了描述的方便，描述以上装置时以功能分为各种单元分别描述。当然，在实施本说明书一个或多个实施例时可以把各单元的功能在同一个或多个软件和/或硬件中实现。

[166]本领域内的技术人员应明白，本说明书的实施例可提供为方法、系统、或计算机程序产品。因此，本说明书一个或多个实施例可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本说明书一个或多个实施例可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质（包括但不限于磁盘存储器、CD-ROM、光学存储器等）上实施的计算机程序产品的形式。

[167]本说明书的实施例是参照根据本说明书实施例的方法、设备（系统）、和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程欺诈案例的串并设备的处理器以产生一个机器，使得通过计算机或其他可编程欺诈案例的串并设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

[168]这些计算机程序指令也可存储在能引导计算机或其他可编程欺诈案例的串并设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能。

[169]这些计算机程序指令也可装载到计算机或其他可编程欺诈案例的串并设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的步骤。

[170]在一个典型的配置中，计算设备包括一个或多个处理器（CPU）、输入/输出接口、网络接口和内存。

[171]内存可能包括计算机可读介质中的非永久性存储器，随机存取存储器（RAM）和/或非易失性内存等形式，如只读存储器（ROM）或闪存（flash RAM）。内存是计算机可读介质的示例。

[172]计算机可读介质包括永久性和非永久性、可移动和非可移动媒体可以由任何方法或技术来实现信息存储。信息可以是计算机可读指令、数据结构、程序的模块或其他数据。计算机的存储介质的例子包括，但不限于相变内存（PRAM）、静态随机存取存储器（SRAM）、动态随机存取存储器（DRAM）、其他类型的随机存取存储器（RAM）、只读存储器（ROM）、电可擦除可编程只读存储器（EEPROM）、快闪记忆体或其他内存技术、只读光盘只读存储器（CD-ROM）、数字多功能光盘（DVD）或其他光学存储、磁盒式磁带，磁带磁磁盘存储或其他磁性存储设备或任何其他非传输介质，可用于存储可以被计算设备访问的信息。按照本文中的界定，计算机可读介质不包括暂存电脑可读媒体（transitory media），如调制的数据信号和载波。

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

[174]本领域技术人员应明白，本说明书的实施例可提供为方法、系统或计算机程序产品。因此，本说明书一个或多个实施例可采用完全硬件实施例、完全软件实施例或结合软件和硬件方面的实施例的形式。而且，本说明书一个或多个实施例可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质（包括但不限于磁盘存储器、CD-ROM、光学存储器等）上实施的计算机程序产品的形式。

[175]本说明书一个或多个实施例可以在由计算机执行的计算机可执行指令的一般上下文中描述，例如程序模块。一般地，程序模块包括执行特定任务或实现特定抽象数据类型的例程、程序、对象、组件、数据结构等等。也可以在分布式计算环境中实践本说明书一个或多个实施例，在这些分布式计算环境中，由通过通信网络而被连接的远程处理设备来执行任务。在分布式计算环境中，程序模块可以位于包括存储设备在内的本地和远程计算机存储介质中。

[176]本说明书中的各个实施例均采用递进的方式描述，各个实施例之间相同相似的部分互相参见即可，每个实施例重点说明的都是与其他实施例的不同之处。尤其，对于系统实施例而言，由于其基本相似于方法实施例，所以描述的比较简单，相关之处参见方法实施例的部分说明即可。

[177]以上所述仅为本说明书的实施例而已，并不用于限制本说明书。对于本领域技术人员来说，本说明书可以有各种更改和变化。凡在本说明书的精神和原理之内所作的任何修改、等同替换、改进等，均应包含在本说明书的权利要求范围之内。

权利要求书

1、一种基于隐私保护的图模型训练方法，应用于终端设备，所述方法包括：

获取待构建的第一图表的节点信息，以及第二图表的节点信息和节点连接信息；

基于所述第一图表的节点信息，通过预设的全连接网络构建所述第一图表，并基于所述第二图表的节点信息和节点连接信息，通过预设的图网络构建所述第二图表，其中，所述全连接网络和所述图网络具有相同的网络参数；

获取所述第一图表中存在训练标签信息的第一节点的隐向量，基于所述第一节点的隐向量和所述第一节点对应的训练标签信息，通过预设的 InstaHide 隐私保护规则构建第一样本数据；

分别为所述第一图表中不存在训练标签信息的第二节点和所述第二图表中的节点生成相应的训练标签信息，获取所述第二节点和所述第二图表中的节点的隐向量，基于所述第二节点和所述第二图表中的节点的隐向量和生成的训练标签信息，通过预设的 InstaHide 隐私保护规则构建第二样本数据；

基于所述第一样本数据和所述第二样本数据对服务器下发的图模型进行模型训练，并获取训练后的图模型对应的梯度信息，将所述梯度信息发送给所述服务器，以使所述服务器基于不同的终端设备提供的梯度信息对所述服务器中的图模型中的模型参数进行更新，得到更新后的图模型。

2、根据权利要求 1 所述的方法，所述全连接网络为全卷积网络 FCN，所述图网络由图卷积神经网络 GCN、图注意力网络 GAT 或 GraphSAGE 构建。

3、根据权利要求 1 所述的方法，所述基于所述第一节点的隐向量和所述第一节点对应的训练标签信息，通过预设的 InstaHide 隐私保护规则构建第一样本数据，包括：

针对所述第一节点的隐向量和所述第一节点对应的训练标签信息，生成所述第一节点对应的置换函数和权重；

基于所述第一节点对应的置换函数和权重，以及所述第一节点的隐向量和所述第一节点对应的训练标签信息，生成第一预选样本数据；

生成所述第一节点对应的节点参数，并基于所述第一节点对应的节点参数和所述第一预选样本数据，生成所述第一样本数据。

4、根据权利要求 3 所述的方法，所述第一节点对应的权重的和为 1。

5、根据权利要求 1 所述的方法，所述基于所述第一样本数据和所述第二样本数据对图模型进行模型训练，并获取训练后的图模型对应的梯度信息，将所述梯度信息发送给服务器，包括：

基于所述第一样本数据对所述图模型进行模型训练，得到所述第一样本数据对应的预设第一分类损失函数的函数值；

基于所述第二样本数据对所述图模型进行模型训练，得到所述第二样本数据对应的预设第二分类损失函数的函数值；

基于所述第一样本数据对应的预设第一分类损失函数的函数值和所述第二样本数据对应的预设第二分类损失函数的函数值，确定所述图模型对应的损失函数的函数值，并基于所述图模型对应的损失函数的函数值，确定训练后的图模型对应的梯度信息，并将所述梯度信息发送给服务器。

6、根据权利要求 5 所述的方法，所述第一分类损失函数和所述第二分类损失函数相同，所述第一分类损失函数为交叉熵损失函数。

7、根据权利要求 1 所述的方法，所述分别为所述第一图表中不存在训练标签信息的第二节点和所述第二图表中的节点生成相应的训练标签信息，包括：

分别将所述第一图表中不存在训练标签信息的第二节点的节点数据和所述第二图表中的节点的节点数据输入到预设的目标图神经网络 GNN 模型中，得到分别与所述第一图表中不存在训练标签信息的第二节点和所述第二图表中的节点相应的训练标签信

息，其中，所述目标GNN模型是基于预设的图表样本进行监督训练得到。

8、根据权利要求1-7中任一项所述的方法，所述图模型为基于图神经网络GNN构建。

9、一种基于隐私保护的图模型训练方法，应用于服务器，所述方法包括：

接收多个不同的终端设备发送的图模型对应的梯度信息，所述图模型对应的梯度信息是所述终端设备基于获取的待构建的第一图表的节点信息，通过预设的全连接网络构建所述第一图表，并基于获取的第二图表的节点信息和节点连接信息，通过预设的图网络构建所述第二图表，基于所述第一图表中存在训练标签信息的第一节点的隐向量和所述第一节点对应的训练标签信息，通过预设的InstaHide隐私保护规则构建第一样本数据，并分别为所述第一图表中不存在训练标签信息的第二节点和所述第二图表中的节点生成相应的训练标签信息，基于所述第二节点和所述第二图表中的节点的隐向量和生成的训练标签信息，通过预设的InstaHide隐私保护规则构建第二样本数据，基于所述第一样本数据和所述第二样本数据对图模型进行模型训练后而得到的梯度信息；

基于多个不同的终端设备发送的图模型对应的梯度信息，对所述图模型中的模型参数进行更新，得到更新后的图模型；

将更新后的图模型发送给所述终端设备，以使所述终端设备基于更新后的图模型执行相应的业务处理。

10、根据权利要求9所述的方法，所述基于多个不同的终端设备发送的图模型对应的梯度信息，对所述图模型中的模型参数进行更新，得到更新后的图模型，包括：

基于多个不同的终端设备发送的图模型对应的梯度信息，通过预设的梯度更新策略对所述图模型中的模型参数进行更新，得到更新后的图模型，所述预设的梯度更新策略包括FedAvg梯度更新策略和FedSgd梯度更新策略中的一种或多种。

11、一种基于隐私保护的图模型训练方法，应用于区块链系统，所述方法包括：

基于预先部署于所述区块链系统中的智能合约向联邦学习框架中的多个不同的终端设备发送图模型的模型参数，所述智能合约用于触发联邦学习处理；

基于所述智能合约，分别从所述多个不同的终端设备获取所述图模型对应的梯度信息，所述图模型对应的梯度信息是所述终端设备基于获取的待构建的第一图表的节点信息，通过预设的全连接网络构建所述第一图表，并基于获取的第二图表的节点信息和节点连接信息，通过预设的图网络构建所述第二图表，基于所述第一图表中存在训练标签信息的第一节点的隐向量和所述第一节点对应的训练标签信息，通过预设的InstaHide隐私保护规则构建第一样本数据，并分别为所述第一图表中不存在训练标签信息的第二节点和所述第二图表中的节点生成相应的训练标签信息，基于所述第二节点和所述第二图表中的节点的隐向量和生成的训练标签信息，通过预设的InstaHide隐私保护规则构建第二样本数据，基于所述第一样本数据和所述第二样本数据对图模型进行模型训练后而得到的梯度信息；

基于多个不同的终端设备发送的图模型对应的梯度信息和所述智能合约，对所述图模型中的模型参数进行更新，得到更新后的图模型；

将更新后的图模型提供给所述终端设备，以使所述终端设备基于更新后的图模型执行相应的业务处理。

12、根据权利要求11所述的方法，所述基于多个不同的终端设备发送的图模型对应的梯度信息和所述智能合约，对所述图模型中的模型参数进行更新，得到更新后的图模型，包括：

基于所述智能合约，从所述区块链系统中获取所述图模型的索引信息，并基于所述索引信息获取所述图模型；

基于多个不同的终端设备发送的图模型对应的梯度信息和所述智能合约，对所述图模型中的模型参数进行更新，得到更新后的图模型；

所述方法还包括：

基于所述索引信息和所述智能合约，将更新后的图模型存储于所述索引信息对应的存储区域。

13、根据权利要求 11 所述的方法，所述基于多个不同的终端设备发送的图模型对应的梯度信息和所述智能合约，对所述图模型中的模型参数进行更新，得到更新后的图模型，包括：

基于所述智能合约，从所述区块链系统中获取所述图模型的索引信息；

基于所述智能合约触发所述索引信息对应存储组件基于多个不同的终端设备发送的图模型对应的梯度信息，对所述图模型中的模型参数进行更新，得到更新后的图模型；

所述将更新后的图模型提供给所述终端设备，包括：

基于所述智能合约触发所述索引信息对应存储组件将更新后的图模型提供给所述终端设备。

14、一种基于隐私保护的图模型训练装置，所述装置包括：

信息获取模块，获取待构建的第一图表的节点信息，以及第二图表的节点信息和节点连接信息；

图表构建模块，基于所述第一图表的节点信息，通过预设的全连接网络构建所述第一图表，并基于所述第二图表的节点信息和节点连接信息，通过预设的图网络构建所述第二图表，其中，所述全连接网络和所述图网络具有相同的网络参数；

第一样本构建模块，获取所述第一图表中存在训练标签信息的第一节点的隐向量，基于所述第一节点的隐向量和所述第一节点对应的训练标签信息，通过预设的 InstaHide 隐私保护规则构建第一样本数据；

第二样本构建模块，分别为所述第一图表中不存在训练标签信息的第二节点和所述第二图表中的节点生成相应的训练标签信息，获取所述第二节点和所述第二图表中的节点的隐向量，基于所述第二节点和所述第二图表中的节点的隐向量和生成的训练标签信息，通过预设的 InstaHide 隐私保护规则构建第二样本数据；

梯度确定模块，基于所述第一样本数据和所述第二样本数据对服务器下发的图模型进行模型训练，并获取训练后的图模型对应的梯度信息，将所述梯度信息发送给所述服务器，以使所述服务器基于不同的终端设备提供的梯度信息对所述服务器中的图模型中的模型参数进行更新，得到更新后的图模型。

15、一种基于隐私保护的图模型训练装置，所述装置包括：

梯度接收模块，接收多个不同的终端设备发送的图模型对应的梯度信息，所述图模型对应的梯度信息是所述终端设备基于获取的待构建的第一图表的节点信息，通过预设的全连接网络构建所述第一图表，并基于获取的第二图表的节点信息和节点连接信息，通过预设的图网络构建所述第二图表，基于所述第一图表中存在训练标签信息的第一节点的隐向量和所述第一节点对应的训练标签信息，通过预设的 InstaHide 隐私保护规则构建第一样本数据，并分别为所述第一图表中不存在训练标签信息的第二节点和所述第二图表中的节点生成相应的训练标签信息，基于所述第二节点和所述第二图表中的节点的隐向量和生成的训练标签信息，通过预设的 InstaHide 隐私保护规则构建第二样本数据，基于所述第一样本数据和所述第二样本数据对图模型进行模型训练后而得到的梯度信息；

模型参数更新模块，基于多个不同的终端设备发送的图模型对应的梯度信息，对所述图模型中的模型参数进行更新，得到更新后的图模型；

发送模块，将更新后的图模型发送给所述终端设备，以使所述终端设备基于更新后的图模型执行相应的业务处理。

16、一种基于隐私保护的图模型训练装置，所述装置为区块链系统中的装置，所述装置包括：

模型参数下发模块，基于预先部署于所述区块链系统中的智能合约向联邦学习框架中的多个不同的终端设备发送图模型的模型参数，所述智能合约用于触发联邦学习处理；

梯度获取模块，基于所述智能合约，分别从所述多个不同的终端设备获取所述图模型对应的梯度信息，所述图模型对应的梯度信息是所述终端设备基于获取的待构建的第一图表的节点信息，通过预设的全连接网络构建所述第一图表，并基于获取的第二图表的节点信息和节点连接信息，通过预设的图网络构建所述第二图表，基于所述第一图表中存在训练标签信息的第一节点的隐向量和所述第一节点对应的训练标签信息，通过预设的 InstaHide 隐私保护规则构建第一样本数据，并分别为所述第一图表中不存在训练标签信息的第二节点和所述第二图表中的节点生成相应的训练标签信息，基于所述第二节点和所述第二图表中的节点的隐向量和生成的训练标签信息，通过预设的 InstaHide 隐私保护规则构建第二样本数据，基于所述第一样本数据和所述第二样本数据对图模型进行模型训练后而得到的梯度信息；

模型参数更新模块，基于多个不同的终端设备发送的图模型对应的梯度信息和所述智能合约，对所述图模型中的模型参数进行更新，得到更新后的图模型；

信息提供模块，将更新后的图模型提供给所述终端设备，以使所述终端设备基于更新后的图模型执行相应的业务处理。

17、一种基于隐私保护的图模型训练设备，所述基于隐私保护的图模型训练设备包括：

处理器；以及

被安排成存储计算机可执行指令的存储器，所述可执行指令在被执行时使所述处理器：

获取待构建的第一图表的节点信息，以及第二图表的节点信息和节点连接信息；

基于所述第一图表的节点信息，通过预设的全连接网络构建所述第一图表，并基于所述第二图表的节点信息和节点连接信息，通过预设的图网络构建所述第二图表，其中，所述全连接网络和所述图网络具有相同的网络参数；

获取所述第一图表中存在训练标签信息的第一节点的隐向量，基于所述第一节点的隐向量和所述第一节点对应的训练标签信息，通过预设的 InstaHide 隐私保护规则构建第一样本数据；

分别为所述第一图表中不存在训练标签信息的第二节点和所述第二图表中的节点生成相应的训练标签信息，获取所述第二节点和所述第二图表中的节点的隐向量，基于所述第二节点和所述第二图表中的节点的隐向量和生成的训练标签信息，通过预设的 InstaHide 隐私保护规则构建第二样本数据；

基于所述第一样本数据和所述第二样本数据对服务器下发的图模型进行模型训练，并获取训练后的图模型对应的梯度信息，将所述梯度信息发送给所述服务器，以使所述服务器基于不同的终端设备提供的梯度信息对所述服务器中的图模型中的模型参数进行更新，得到更新后的图模型。

18、一种基于隐私保护的图模型训练设备，所述基于隐私保护的图模型训练设备包括：

处理器；以及

被安排成存储计算机可执行指令的存储器，所述可执行指令在被执行时使所述处理器：

接收多个不同的终端设备发送的图模型对应的梯度信息，所述图模型对应的梯度信息是所述终端设备基于获取的待构建的第一图表的节点信息，通过预设的全连接网络构建所述第一图表，并基于获取的第二图表的节点信息和节点连接信息，通过预设的图网络构建所述第二图表，基于所述第一图表中存在训练标签信息的第一节点的隐向量和所述第一节点对应的训练标签信息，通过预设的 InstaHide 隐私保护规则构建第一样本数

据，并分别为所述第一图表中不存在训练标签信息的第二节点和所述第二图表中的节点生成相应的训练标签信息，基于所述第二节点和所述第二图表中的节点的隐向量和生成的训练标签信息，通过预设的 InstaHide 隐私保护规则构建第二样本数据，基于所述第一样本数据和所述第二样本数据对图模型进行模型训练后而得到的梯度信息；

基于多个不同的终端设备发送的图模型对应的梯度信息，对所述图模型中的模型参数进行更新，得到更新后的图模型；

将更新后的图模型发送给所述终端设备，以使所述终端设备基于更新后的图模型执行相应的业务处理。

19、一种基于隐私保护的图模型训练设备，所述设备为区块链系统中的设备，所述基于隐私保护的图模型训练设备包括：

处理器；以及

被安排成存储计算机可执行指令的存储器，所述可执行指令在被执行时使所述处理器：

基于预先部署于所述区块链系统中的智能合约向联邦学习框架中的多个不同的终端设备发送图模型的模型参数，所述智能合约用于触发联邦学习处理；

基于所述智能合约，分别从所述多个不同的终端设备获取所述图模型对应的梯度信息，所述图模型对应的梯度信息是所述终端设备基于获取的待构建的第一图表的节点信息，通过预设的全连接网络构建所述第一图表，并基于获取的第二图表的节点信息和节点连接信息，通过预设的图网络构建所述第二图表，基于所述第一图表中存在训练标签信息的第一节点的隐向量和所述第一节点对应的训练标签信息，通过预设的 InstaHide 隐私保护规则构建第一样本数据，并分别为所述第一图表中不存在训练标签信息的第二节点和所述第二图表中的节点生成相应的训练标签信息，基于所述第二节点和所述第二图表中的节点的隐向量和生成的训练标签信息，通过预设的 InstaHide 隐私保护规则构建第二样本数据，基于所述第一样本数据和所述第二样本数据对图模型进行模型训练后而得到的梯度信息；

基于多个不同的终端设备发送的图模型对应的梯度信息和所述智能合约，对所述图模型中的模型参数进行更新，得到更新后的图模型；

将更新后的图模型提供给所述终端设备，以使所述终端设备基于更新后的图模型执行相应的业务处理。

20、一种存储介质，所述存储介质用于存储计算机可执行指令，所述可执行指令在被执行时实现以下流程：

获取待构建的第一图表的节点信息，以及第二图表的节点信息和节点连接信息；

基于所述第一图表的节点信息，通过预设的全连接网络构建所述第一图表，并基于所述第二图表的节点信息和节点连接信息，通过预设的图网络构建所述第二图表，其中，所述全连接网络和所述图网络具有相同的网络参数；

获取所述第一图表中存在训练标签信息的第一节点的隐向量，基于所述第一节点的隐向量和所述第一节点对应的训练标签信息，通过预设的 InstaHide 隐私保护规则构建第一样本数据；

分别为所述第一图表中不存在训练标签信息的第二节点和所述第二图表中的节点生成相应的训练标签信息，获取所述第二节点和所述第二图表中的节点的隐向量，基于所述第二节点和所述第二图表中的节点的隐向量和生成的训练标签信息，通过预设的 InstaHide 隐私保护规则构建第二样本数据；

基于所述第一样本数据和所述第二样本数据对服务器下发的图模型进行模型训练，并获取训练后的图模型对应的梯度信息，将所述梯度信息发送给所述服务器，以使所述服务器基于不同的终端设备提供的梯度信息对所述服务器中的图模型中的模型参数进行更新，得到更新后的图模型。

21、一种存储介质，所述存储介质用于存储计算机可执行指令，所述可执行指令在被执行时实现以下流程：

接收多个不同的终端设备发送的图模型对应的梯度信息，所述图模型对应的梯度信息是所述终端设备基于获取的待构建的第一图表的节点信息，通过预设的全连接网络构建所述第一图表，并基于获取的第二图表的节点信息和节点连接信息，通过预设的图网络构建所述第二图表，基于所述第一图表中存在训练标签信息的第一节点的隐向量和所述第一节点对应的训练标签信息，通过预设的 InstaHide 隐私保护规则构建第一样本数据，并分别为所述第一图表中不存在训练标签信息的第二节点和所述第二图表中的节点生成相应的训练标签信息，基于所述第二节点和所述第二图表中的节点的隐向量和生成的训练标签信息，通过预设的 InstaHide 隐私保护规则构建第二样本数据，基于所述第一样本数据和所述第二样本数据对图模型进行模型训练后而得到的梯度信息；

基于多个不同的终端设备发送的图模型对应的梯度信息，对所述图模型中的模型参数进行更新，得到更新后的图模型；

将更新后的图模型发送给所述终端设备，以使所述终端设备基于更新后的图模型执行相应的业务处理。

22、一种存储介质，所述存储介质用于存储计算机可执行指令，所述可执行指令在被执行时实现以下流程：

基于预先部署于区块链系统中的智能合约向联邦学习框架中的多个不同的终端设备发送图模型的模型参数，所述智能合约用于触发联邦学习处理；

基于所述智能合约，分别从所述多个不同的终端设备获取所述图模型对应的梯度信息，所述图模型对应的梯度信息是所述终端设备基于获取的待构建的第一图表的节点信息，通过预设的全连接网络构建所述第一图表，并基于获取的第二图表的节点信息和节点连接信息，通过预设的图网络构建所述第二图表，基于所述第一图表中存在训练标签信息的第一节点的隐向量和所述第一节点对应的训练标签信息，通过预设的 InstaHide 隐私保护规则构建第一样本数据，并分别为所述第一图表中不存在训练标签信息的第二节点和所述第二图表中的节点生成相应的训练标签信息，基于所述第二节点和所述第二图表中的节点的隐向量和生成的训练标签信息，通过预设的 InstaHide 隐私保护规则构建第二样本数据，基于所述第一样本数据和所述第二样本数据对图模型进行模型训练后而得到的梯度信息；

基于多个不同的终端设备发送的图模型对应的梯度信息和所述智能合约，对所述图模型中的模型参数进行更新，得到更新后的图模型；

将更新后的图模型提供给所述终端设备，以使所述终端设备基于更新后的图模型执行相应的业务处理。