

联邦学习方法、装置、可读存储介质及电子设备

技术领域

[01]本申请涉及机器学习算法领域，更具体地涉及一种联邦学习方法、装置、可读存储介质及电子设备。

背景技术

[02]梯度交换是现代多机训练（例如分布式训练、联邦学习等）常用的通讯方式，即各个设备根据本地的训练数据得到待训练模型的梯度，然后各自将梯度共享，并进行梯度融合，采用融合后的梯度更新待训练模型。但是，在共享梯度的过程中，攻击者可能通过网络流量监听或者加密流量劫持等方式获取到明文的梯度信息，然后根据梯度信息获取到对应设备的隐私的训练数据，从而导致隐私泄露。

发明内容

[03]本申请的目的之一在于提供一种联邦学习方法，基于安全切面，在各联邦学习设备向联邦学习服务器发送明文梯度时，对其进行拦截和加密，并将加密后的密文梯度发送至联邦学习服务器，避免攻击者获得明文梯度而导致隐私泄漏。

[04]基于上述目的，本申请一方面提供一种联邦学习方法，应用于联邦学习设备，其包括以下步骤：联邦学习设备通过预先部署的切面底座，根据预设的第一切点和第一切面程序，在所述联邦学习设备的梯度发送函数处注入所述第一切面程序；所述联邦学习设备根据本地的训练数据对待训练模型进行训练，得到所述待训练模型的明文梯度，并通过所述梯度发送函数向联邦学习服务器发送所述明文梯度；通过所述第一切面程序拦截所述梯度发送函数发送的明文梯度，并对所述明文梯度进行加密，得到密文梯度，将所述密文梯度发送给所述联邦学习服务器，以使所述联邦学习服务器对接收到的各联邦学习设备发送的密文梯度进行解密，并根据解密后得到的各明文梯度更新所述待训练模型的参数。

[05]进一步地，在一些实施方式中，所述联邦学习方法还包括：在联邦学习前，所述联邦学习设备对切面服务器的可信执行环境进行远程认证，认证通过后，与所述可信执行环境建立可信的安全传输层协议连接；接收通过所述可信执行环境生成的加密密钥。

[06]进一步地，在一些实施方式中，所述联邦学习服务器对接收到的各联邦学习设备发送的密文梯度进行解密，具体包括：所述联邦学习服务器通过梯度接收函数接收所述密文梯度；通过预先注入在所述梯度接收函数处的第二切面程序拦截所述密文梯度，并对所述密文梯度进行解密。

[07]本申请的另一目的在于提供一种联邦学习方法，联邦学习服务器接收各联邦学习设备的加密后的密文梯度，并对其进行解密，得到解密后的明文梯度，以避免明文梯度在传输过程中被攻击者获取而导致隐私泄露。

[08]基于上述目的，本申请另一方面提供一种联邦学习方法，应用于联邦学习服务器，其包括以下步骤：联邦学习服务器通过预先部署的切面底座，根据预设的第二切点和第二切面程序，在所述联邦学习服务器的梯度接收函数处注入第二切面程序；通过所述梯度接收函数接收各联邦学习设备发送的待训练模型的密文梯度；通过所述第二切面程序拦截所述密文梯度，并对所述密文梯度进行解密，得到明文梯度；根据各联邦学习设备的明文梯度更新各联邦学习设备的待训练模型的参数。

[09]进一步地，在一些实施方式中，所述联邦学习方法还包括：在联邦学习前，对切面服务器的可信执行环境进行远程认证，认证通过后，与所述可信执行环境建立可信的安全传输层协议连接；接收通过所述可信执行环境生成的解密密钥。

[10]本申请又一目的在于提供一种联邦学习装置，基于安全切面，在各联邦学习设备向联邦学习服务器发送明文梯度时，对其进行拦截和加密，并将加密后的密文梯度发送至联邦学习服务器，避免攻击者获得明文梯度而导致隐私泄漏。

[11]基于上述目的，本申请又一方面提供一种联邦学习装置，所述装置应用于联邦学习设备，所述装置包括：注入模块，设置为通过预先部署的切面底座，根据预设的第一切点和第一切面程序，在所述联邦学习设备的梯度发送函数处注入所述第一切面程序；训练模块，设置为根据本地的训练数据对待训练模型进行训练，得到所述待训练模型的明文梯度，并通过所述梯度发送函数向联邦学习服务器发送所述明文梯度；加密模块，设置为通过所述第一切面程序拦截所述梯度发送函数发送的明文梯度，并对所述明文梯度进行加密，得到密文梯度，将所述密文梯度发送给所述联邦学习服务器，以使所述联邦学习服务器对接收到的各联邦学习设备发送的密文梯度进行解密，并根据解密后得到的各明文梯度更新所述待训练模型的参数。

[12]进一步地，在一些实施方式中，所述联邦学习装置还包括连接模块，所述连接模块

设置为在联邦学习前，所述联邦学习设备对切面服务器的可信执行环境进行远程认证，认证通过后，与所述可信执行环境建立可信的安全传输层协议连接；然后接收通过所述可信执行环境生成的加密密钥。

[13]进一步地，在一些实施方式中，所述联邦学习服务器对接收到的各联邦学习设备发送的密文梯度进行解密，具体包括：所述联邦学习服务器通过梯度接收函数接收所述密文梯度；通过预先注入在所述梯度接收函数处的第二切面程序拦截所述密文梯度，并对所述密文梯度进行解密。

[14]本申请又一目的在于提供一种联邦学习装置，联邦学习服务器接收各联邦学习设备的加密后的密文梯度，并对其进行解密，得到解密后的明文梯度，以避免明文梯度在传输过程中被攻击者获取而导致隐私泄露。

[15]基于上述目的，本申请又一方面提供一种联邦学习装置，所述装置应用于联邦学习服务器，所述装置包括：注入模块，设置为通过预先部署的切面底座，根据预设的第二切点和第二切面程序，在所述联邦学习服务器的梯度接收函数处注入第二切面程序；接收模块，设置为通过所述梯度接收函数接收各联邦学习设备发送的待训练模型的密文梯度；解密模块，设置为通过所述第二切面程序拦截所述密文梯度，并对所述密文梯度进行解密，得到明文梯度；更新模块，设置为根据各联邦学习设备的明文梯度更新各联邦学习设备的待训练模型的参数。

[16]进一步地，在一些实施方式中，所述联邦学习装置还包括连接模块，所述连接模块设置为在联邦学习前，对切面服务器的可信执行环境进行远程认证，认证通过后，与所述可信执行环境建立可信的安全传输层协议连接；然后接收通过所述可信执行环境生成的解密密钥。

[17]本申请又一目的在于提供一种可读存储介质，其上存储有计算机程序，当计算机程序在计算机中执行时，令计算机执行如上所述的联邦学习方法的步骤。

[18]本申请又一目的在于提供一种电子设备，其包括存储器和处理器，存储器中存储有可执行代码，当处理器执行可执行代码时，其执行如上所述的联邦学习方法的步骤。

附图说明

[19]图 1 为根据本申请一实施例的联邦学习方法的流程图。

[20]图 2 为根据本申请另一实施例的联邦学习方法的流程图。

[21]图 3 为根据本申请又一实施例的联邦学习装置的结构框图。

[22]图 4 为根据本申请又一实施例的联邦学习装置的结构框图。

具体实施方式

[23]下面结合附图，给出本申请的较佳实施例，并予以详细描述。

[24]安全切面是指通过采用面向切面编程 (Aspect-oriented Programming, AOP) 的方式，在不修改业务应用程序的情况下，在业务应用程序的运行逻辑中动态的添加或修改用于实现安全切面业务的切面程序的方法。使得在实现安全切面业务的同时，使实现安全切面业务的程序与业务应用程序解耦，从而避免高耦合导致的开发迭代问题。

[25]这里说的切面程序，即基于业务运行逻辑来实现安全切面业务的增强程序。可通过采用面向切面编程的方式，将切面程序注入至业务应用程序的相应切点处，该切面程序在执行业务应用程序的过程中被触发执行，实现所需的安全切面业务功能。

[26]而业务应用程序在执行业务时，业务应用程序通常通过方法之间的调用进行业务执行。因此，可将业务应用程序中的任意方法作为切面程序的切入点，即上述所说的切点，并将切面程序注入对应切点。使得业务应用程序在执行至切点，即调用该切点对应的业务应用程序的方法时，执行在该切点注入的切面程序。

[27]通常，负责将切面程序注入至切点的过程的代码存在较高的可复用性，因此，通常将实现这一过程的程序抽象为一个服务模块，即切面底座。切面底座可从提供安全切面业务的服务器获取需要部署的切面程序以及获取切面程序在业务应用程序中注入的切点，在应用容器启动后被唤醒并在业务应用程序的切点处注入对应的切面程序。

[28]业务应用程序可以是业务平台的服务器中提供业务服务的业务应用程序。其中，业务服务可以是业务平台的服务器向用户提供的业务服务，如，查询业务、支付业务等。业务服务还可以是业务平台的某服务器向其他服务器提供的业务服务，如，结算业务等。

[29]当然了，由上述描述可知，为了使安全切面业务的程序与业务应用程序解耦，本说明书通过采用面向切面编程的方式使得安全切面业务的程序与业务应用程序在业务执行时相互交织，但又互相平行可各自独立维护。因此，区别于业务应用程序的业务提供方，提供安全切面业务的第三方可通过服务器管理安全切面业务所涉及的内容，例如，安全切面业务管控策略的配置、切面程序的版本迭代、切面程序的部署规则配置等等。当然，提供安全切面业务的可以是第三方，也可以是业务提供方。

[30]服务器在管理安全切面业务所涉及的内容时，可通过配置文件记录各种配置信息，例如各种策略的配置、切面程序的部署规则配置等。使得切面底座可根据配置文件完成对切面程序的部署，或者服务器可根据配置文件实现安全切面业务。

[31]在实际应用中，业务提供方通常设置有包括若干物理机或物理服务器的机房，通过物理机提供业务应用程序所需的物理资源。当然，一个业务应用程序可能无需整个物理机的所有物理资源，于是，一般还会通过虚拟化技术在一个物理机上运行多个虚拟主机（virtual hosting）。各个虚拟主机之间是互相独立的，各自享有物理机的部分物理资源。然后，可在虚拟主机中部署应用容器，并通过应用容器运行业务应用程序。应用容器通常包含分配给该应用容器的物理资源，如 CPU、内存等，以及提供给该应用容器的运行环境，如操作系统（Operating System, OS）或其他运行环境数据，如，容器的序列（Serial Number, SN）号、分配的 IP（Influential Property）、应用名、租户、环境变量等）。业务应用程序可部署在应用容器中以执行业务。

[32]而在基于安全切面执行业务的场景中，业务提供方或者提供安全切面业务的第三方的服务器可提供服务器，通过服务器管理安全切面业务所涉及的内容，并将切面底座部署在应用容器中，通过切面底座将切面程序注入业务应用程序中的业务应用程序中，以为业务提供方的应用容器提供安全切面业务的支持。

[33]于是，可预先在业务提供方的应用容器中部署切面底座。一般情况下，在启动应用容器时，可唤起提供给应用容器的操作系统，以及运行预先部署的切面底座，通过切面底座从服务器中得到切面程序和业务应用程序的切点，并将切面程序注入应用容器中的业务应用程序的切点处。此外，切面底座也可在业务应用程序执行过程中，从服务器中得到切面程序和业务应用程序的切点，并将切面程序注入应用容器中的业务应用程序的切点处。

[34]当然，切面底座如何从服务器中得到部署切面程序所需的信息，可根据需要设置。例如，可以是根据配置文件主动从服务器中拉取所需的信息，或者服务器可主动下发使切面底座接收所需的信息。

[35]将切面程序注入业务应用程序的切点后，业务应用程序在执行过程中，即可触发该切面程序从而实现相应的安全切面业务功能。

[36]联邦学习是一种分布式机器学习技术，其核心思想是通过多个拥有本地数据的数据源之间进行分布式模型训练，在不需要交换本地个体或样本数据的前提下，仅通过交换

模型参数或中间结果的方式，构件基于虚拟融合数据下的全局模型，从而实现数据隐私保护和数据共享计算的平衡，即“数据可用不可见”、“数据不动模型动”的应用新范式。参与联邦学习的包括一个联邦学习服务器和至少两个联邦学习设备，联邦学习设备上具有本地的训练数据，联邦学习设备可根据本地的训练数据对待训练模型进行训练，得到梯度，然后将梯度发送至联邦学习服务器，联邦学习服务器根据各联邦学习设备的梯度进行梯度融合，然后将融合后的梯度发送回各联邦学习设备，各联邦学习设备根据融合后的梯度更新待训练模型的参数。这样，在训练过程中，各设备的训练数据始终保存在本地，只需将待训练模型的梯度上传至联邦学习服务器中进行融合，因此可以很好地保护隐私的训练数据。

[37]但是，在最新的研究中发现，隐私的训练数据可以通过其梯度来获取，其被称为深度梯度泄露。在联邦学习过程中，攻击者可能会通过网络流量监听或者加密流量劫持等方式，获取到各联邦学习设备发送至联邦学习服务器的明文梯度，然后通过明文梯度获取到各联邦学习设备上的训练数据，导致隐私泄露。

[38]由此，本申请提供一种联邦学习方法，基于安全切面，在各联邦学习设备向联邦学习服务器发送明文梯度时，对其进行拦截和加密，并将加密后的密文梯度发送至联邦学习服务器，在联邦学习服务器接收到密文梯度时，对其进行拦截和解密，得到明文梯度，从而根据各联邦学习设备的明文梯度进行融合并更新模型参数，这样可以有效地抵御攻击者通过网络监听或者中间人攻击的方式获取明文梯度，避免隐私的训练数据泄露；且本申请的联邦学习方法不需要在联邦学习框架的代码层面进行二次开发，对原有的业务不存在入侵性，维护成本低；此外，本申请的方法不需要重新训练模型，也不影响模型的准确度。

[39]如图 1 所示，本申请一实施例提供一种联邦学习方法，应用于联邦学习设备，其包括步骤 110 至步骤 130。

[40]110: 联邦学习设备通过预先部署的切面底座，根据预设的第一切点和第一切面程序，在联邦学习设备的梯度发送函数处注入第一切面程序。

[41]联邦学习设备上预先部署有切面底座，在联邦学习开始后，切面底座可以根据第一切点和第一切面程序，在联邦学习设备的梯度发送函数处注入第一切面程序。梯度发送函数是用于将联邦学习设备的梯度向联邦学习服务器发送的函数，将其作为第一切点，并注入第一切面程序后，当联邦学习设备通过梯度发送函数向联邦学习服务器发送明文梯度时，第一切面程序会执行预设的逻辑，从而实现预设的业务。

[42]在一些实施例中，第一切点和第一切面程序可以是预先存储在联邦学习设备中的，当联邦学习开始后，切面底座将启动，并根据预设的第一切点和第一切面程序完成切点注入。在另外一些实施例中，第一切点和第一切面程序可以由切面服务器下发，当联邦学习开始后，切面服务器将第一切点和第一切面程序下发至切面底座，切面底座则根据接收到的第一切点和第一切面程序完成切点注入。

[43]120: 联邦学习设备根据本地的训练数据对待训练模型进行训练，得到待训练模型的明文梯度，并通过梯度发送函数向联邦学习服务器发送明文梯度。

[44]130: 通过第一切面程序拦截梯度发送函数发送的明文梯度，并对明文梯度进行加密，得到密文梯度，将密文梯度发送给联邦学习服务器，以使联邦学习服务器对接收到的各联邦学习设备发送的密文梯度进行解密，并根据解密后得到的各明文梯度更新待训练模型的参数。

[45]在联邦学习设备通过梯度发送函数向联邦学习服务器发送明文梯度时，第一切面程序将对其进行拦截，然后对拦截到的明文梯度进行加密，得到密文梯度，然后将密文梯度发送给联邦学习服务器，联邦学习服务器接收到密文梯度后，将对密文梯度进行解密，重新得到明文梯度，从而根据各联邦学习设备的明文梯度更新待训练模型的参数。由于联邦学习设备传输的是密文梯度，即使在上传过程中被泄露，攻击者也无法根据密文梯度得到明文梯度，也就无法由明文梯度获得联邦学习设备的隐私的训练数据，从而可以更好地保护隐私。

[46]本申请的联邦学习方法通过注入在梯度发送函数处的第一切面程序对明文梯度进行加密，因此不需要对原有的联邦学习框架进行修改，对联邦学习业务不存在入侵性，维护成本低。

[47]在一些实施例中，在联邦学习前，可以先生成加密密钥和解密密钥，从而采用加密密钥对明文梯度进行加密，得到密文梯度，并采用解密密钥对密文梯度进行解密，重新得到明文梯度。在一个联邦学习任务中，加密密钥和解密密钥全局唯一。

[48]在一些实施例中，加密密钥和解密密钥可通过切面服务器的可信执行环境生成。切面服务器生成加密密钥和解密密钥后，可将加密密钥发送至联邦学习设备，以用于对明文梯度进行加密。在将加密密钥发送至联邦学习设备前，联邦学习设备可先认证切面服务器的可信执行环境是否可信，认证通过后，再与切面服务器的可信执行环境建立可信的安全传输层协议（TLS）连接，以保证在传输过程中加密密钥的安全性。

[49]在一些实施例中，切面服务器的可信执行环境可以是基于 Inter SGX 的可信执行环境。Inter SGX，即 Inter Software Guard extensions，英特尔软件保护扩展，是一种旨在以硬件安全为强制性保障，不依赖于固件和软件的安全状态的安全机制。Inter SGX 实际上是一组 CPU 指令扩展，可创建一个可信执行环境来保护代码和数据，即使 root 权限也无法访问，这样应用程序可以使用它来隔离代码和数据的特定可信区域，保障其机密性和完整性不受恶意软件的破坏。Inter SGX 提供的可信执行环境也可称之为 enclave（飞地），用于存放需保护的代码和数据。

[50]在与基于 SGX 的可信执行环境进行通信前，联邦学习设备还需要完成对可信执行环境的远程认证。为了实现远程认证，切面服务器还需要引入一个特殊的 quoting enclave（QE）。在联邦学习服务器对切面服务器的可信执行环境进行远程认证时，可信执行环境先执行 EREPORT 指令，将可信执行环境的身份和附加信息组合生成报告结构，并将报告结构传给 QE，QE 调用 EGETKEY 来获取报告密钥并验证该报告结构，判断该可信执行环境是否运行于同一平台，如果成功，QE 将生成一个加密的引用结构体 QUOTE，并使用 EPID 进行签名，然后将 QUOTE 和签名一起发送给联邦学习设备；由于 QUOTE 是加密的，只能由英特尔来验证，因此联邦学习设备会将其发送至 Inter Attestation Service（IAS），IAS 会对其进行验证，并返回一个认证报告，该认证报告表明可信执行环境是可信的；联邦学习设备接收到认证报告并校验通过后，说明认证通过，将与可信执行环境建立可信的 TLS 连接。

[51]联邦学习服务器具有梯度接收函数，用于接收联邦学习设备的梯度，当联邦学习设备将密文梯度发送至联邦学习服务器时，联邦学习服务器将通过梯度接收函数接收密文梯度。

[52]在联邦学习开始前，联邦学习服务器可通过预先部署的切面底座，根据预设的第二切点和第二切面程序，在联邦学习服务器的梯度接收函数处注入第二切面程序。在联邦学习服务器通过梯度接收函数接收密文梯度时，第二切面程序将拦截密文梯度，并对其进行解密，从而得到对应的明文梯度。

[53]联邦学习服务器可采用通过切面服务器的可信执行环境生成的解密密钥对密文梯度进行解密。与联邦学习设备相同，在接收解密密钥前，联邦学习服务器需要先对切面服务器的可信执行环境进行远程认证，认证通过后，再建立可信的 TLS 连接。

[54]本申请实施例的联邦学习方法，对联邦学习设备的明文梯度进行加密，并将加密后的密文梯度发送至联邦学习服务器，可避免明文梯度被攻击者获取而导致隐私泄露；基

于安全切面，在联邦学习设备的梯度发送函数处注入第一切面程序，并通过第一切面程序对明文梯度进行拦截和加密，不需要对原有的联邦学习框架进行修改，对联邦学习业务不存在入侵性，维护成本低；通过切面服务器的可信执行环境生成加密密钥和解密密钥，保证它们不被攻击者窃取和伪造。

[55]如图 2 所示，本申请另一实施例提供一种联邦学习方法，应用于联邦学习服务器，该方法包括步骤 210 至步骤 240。

[56]210: 联邦学习服务器通过预先部署的切面底座，根据预设的第二切点和第二切面程序，在联邦学习服务器的梯度接收函数处注入第二切面程序。

[57]联邦学习服务器上预先部署有切面底座，在联邦学习开始后，切面底座可以根据第二切点和第二切面程序，在联邦学习服务器的梯度接收函数处注入第二切面程序。梯度接收函数是用于接收各联邦学习设备的待训练模型的梯度的函数，当联邦学习设备向联邦学习服务器发送梯度时，联邦学习服务器将通过梯度接收函数接收梯度。将梯度接收函数作为第二切点，并注入第二切面程序后，当联邦学习服务器通过接收梯度函数接收联邦学习设备的密文梯度时，第二切面程序会执行预设的逻辑，从而实现预设的业务。

[58]在一些实施例中，第二切点和第二切面程序可以是预先存储在联邦学习服务器中的，当联邦学习开始后，切面底座将启动，并根据预设的第二切点和第二切面程序完成切点注入。在另外一些实施例中，第二切点和第二切面程序可以由切面服务器下发，当联邦学习开始后，切面服务器将第二切点和第二切面程序下发至切面底座，切面底座则根据接收到的第二切点和第二切面程序完成切点注入。

[59]220: 通过梯度接收函数接收各联邦学习设备发送的待训练模型的密文梯度。

[60]在联邦学习开始后，各联邦学习设备会通过预先部署的切面底座，根据预设的第一切点和第一切面程序，在联邦学习设备的梯度发送函数处注入第一切面程序；然后各联邦学习设备会分别根据本地的训练数据对待训练模型进行训练，然后得到待训练模型的明文梯度，并通过梯度发送函数向联邦学习服务器发送明文梯度，第一切面程序将拦截明文梯度，并对明文梯度进行加密，得到密文梯度，然后各联邦学习设备将各自的密文梯度发送至联邦学习服务器，联邦学习服务器将通过梯度接收函数接收各联邦学习设备的密文梯度。

[61]由于联邦学习服务器接收到的是密文梯度，因此可以避免攻击者获得明文梯度而导致隐私泄露。

- [62]230: 通过第二切面程序拦截密文梯度, 并对密文梯度进行解密, 得到明文梯度。
- [63]在梯度接收函数接收密文梯度时, 第二切面程序将拦截密文梯度, 并对其进行解密, 得到对应的明文梯度, 由于第二切面程序是注入在梯度接收函数处, 其并不会对原有的联邦学习框架进行修改, 对联邦学习业务不存在入侵性, 维护成本低。
- [64]由于联邦学习设备可能有多个, 因此对每个联邦学习设备的密文梯度, 均需要通过第二切面程序进行拦截并解密, 从而得到各联邦学习设备的明文梯度。
- [65]在一些实施例中, 在联邦学习前, 可以先生成加密密钥和解密密钥, 从而使联邦学习设备采用加密密钥对明文梯度进行加密, 得到密文梯度, 联邦学习服务器则采用解密密钥对密文梯度进行解密, 重新得到明文梯度。在一个联邦学习任务中, 加密密钥和解密密钥全局唯一。
- [66]在一些实施例中, 加密密钥和解密密钥可通过切面服务器的可信执行环境生成。切面服务器生成加密密钥和解密密钥后, 可将加密密钥发送至各联邦学习设备, 以用于对明文梯度进行加密, 并将解密密钥发送至联邦学习服务器, 以用于对密文梯度进行解密。在发送加密密钥和解密密钥前, 各联邦学习设备和联邦学习服务器可先认证切面服务器的可信执行环境是否可信, 认证通过后, 再与切面服务器的可信执行环境建立可信的安全传输层协议(TLS)连接, 通过 TLS 连接传输加密密钥和解密密钥, 以保证在传输过程中加密密钥和解密密钥的安全性。
- [67]在一些实施例中, 切面服务器的可信执行环境可以是基于 Inter SGX 的可信执行环境。在与其进行通信前, 联邦学习服务器还需要完成对可信执行环境的远程认证, 远程认证过程与联邦学习设备相同, 此处不再赘述。
- [68]240: 根据各联邦学习设备的明文梯度更新各联邦学习设备的待训练模型的参数。
- [69]得到各联邦学习设备的明文梯度后, 联邦学习服务器将对它们进行梯度融合, 得到融合后的梯度, 然后根据融合后的梯度更新各联邦学习设备的待训练模型的参数。
- [70]本申请实施例的联邦学习方法, 联邦学习服务器接收各联邦学习设备的加密后的密文梯度, 并对其进行解密, 得到解密后的明文梯度, 以避免明文梯度在传输过程中被攻击者获取而导致隐私泄露; 基于安全切面, 在联邦学习服务器的梯度接收函数处注入第二切面程序, 并通过第二切面程序对密文梯度进行拦截和解密, 不需要对原有的联邦学习框架进行修改, 对联邦学习业务不存在入侵性, 维护成本低; 通过切面服务器的可信执行环境生成加密密钥和解密密钥, 保证它们不被攻击者窃取和伪造。

[71]如图 3 所示,本申请又一实施例提供一种联邦学习装置,其应用于联邦学习设备,包括相互数据通信的注入模块 11、训练模块 12 和加密模块 13。

[72]注入模块 11 设置为通过预先部署的切面底座,根据预设的第一切点和第一切面程序,在联邦学习设备的梯度发送函数处注入第一切面程序。

[73]联邦学习设备上预先部署有切面底座,在联邦学习开始后,注入模块 11 可通过切面底座根据第一切点和第一切面程序,在联邦学习设备的梯度发送函数处注入第一切面程序。梯度发送函数是用于将联邦学习设备的梯度向联邦学习服务器发送的函数,将其作为第一切点,并注入第一切面程序后,当联邦学习设备通过梯度发送函数向联邦学习服务器发送明文梯度时,第一切面程序会执行预设的逻辑,从而实现预设的业务。

[74]在一些实施例中,第一切点和第一切面程序可以是预先存储在联邦学习设备中的,当联邦学习开始后,切面底座将启动,并根据预设的第一切点和第一切面程序完成切点注入。在另外一些实施例中,第一切点和第一切面程序可以由切面服务器下发,当联邦学习开始后,切面服务器将第一切点和第一切面程序下发至切面底座,注入模块 11 通过切面底座完成切点注入。

[75]训练模块 12 设置为根据本地的训练数据对待训练模型进行训练,得到待训练模型的明文梯度,并通过梯度发送函数向联邦学习服务器发送明文梯度。

[76]加密模块 13 设置为通过第一切面程序拦截梯度发送函数发送的明文梯度,并对明文梯度进行加密,得到密文梯度,将密文梯度发送给联邦学习服务器,以使联邦学习服务器对接收到的各联邦学习设备发送的密文梯度进行解密,并根据解密后得到的各明文梯度更新待训练模型的参数。

[77]在注入模块 11 通过梯度发送函数向联邦学习服务器发送明文梯度时,加密模块 13 将通过第一切面程序对其进行拦截,然后对拦截到的明文梯度进行加密,得到密文梯度,然后将密文梯度发送给联邦学习服务器,联邦学习服务器接到密文梯度后,将对密文梯度进行解密,重新得到明文梯度,从而根据各联邦学习设备的明文梯度更新待训练模型的参数。由于传输的是密文梯度,即使其在上传过程中被泄露,攻击者也无法根据密文梯度得到明文梯度,也就无法由明文梯度获得联邦学习设备的隐私的训练数据,从而可以更好地保护隐私。

[78]加密模块 13 通过注入在梯度发送函数处的第一切面程序对明文梯度进行加密,因此不需要对原有的联邦学习框架进行修改,对联邦学习业务不存在入侵性,维护成本低。

[79]在一些实施例中，在联邦学习前，可以先生成加密密钥和解密密钥，从而采用加密密钥对明文梯度进行加密，得到密文梯度，并采用解密密钥对密文梯度进行解密，重新得到明文梯度。在一个联邦学习任务中，加密密钥和解密密钥全局唯一。

[80]在一些实施例中，加密密钥和解密密钥可通过切面服务器的可信执行环境生成。切面服务器生成加密密钥和解密密钥后，可将加密密钥发送至联邦学习设备，以用于对明文梯度进行加密。在将加密密钥发送至联邦学习设备前，联邦学习设备可先认证切面服务器的可信执行环境是否可信，认证通过后，再与切面服务器的可信执行环境建立可信的安全传输层协议（TLS）连接，以保证在传输过程中加密密钥的安全性。因此，联邦学习装置还可以包括连接模块，其设置为在联邦学习前，对切面服务器的可信执行环境进行远程认证，认证通过后，与所述可信执行环境建立可信的 TLS 连接；然后接收通过所述可信执行环境生成的加密密钥。

[81]在一些实施例中，切面服务器的可信执行环境可以是基于 Inter SGX 的可信执行环境。

[82]联邦学习服务器具有梯度接收函数，用于接收联邦学习设备的梯度，当加密模块 13 将密文梯度发送至联邦学习服务器时，联邦学习服务器将通过梯度接收函数接收密文梯度。

[83]在联邦学习开始前，联邦学习服务器可通过预先部署的切面底座，根据预设的第二切点和第二切面程序，在联邦学习服务器的梯度接收函数处注入第二切面程序。在联邦学习服务器通过梯度接收函数接收密文梯度时，第二切面程序将拦截密文梯度，并对其进行解密，从而得到对应的明文梯度。

[84]联邦学习服务器可采用通过切面服务器的可信执行环境生成的解密密钥对密文梯度进行解密。与联邦学习设备相同，在接收解密密钥前，联邦学习服务器需要先对切面服务器的可信执行环境进行远程认证，认证通过后，再建立可信的 TLS 连接。

[85]本申请实施例的联邦学习装置，通过加密模块 13 对明文梯度进行加密，并将加密后的密文梯度发送至联邦学习服务器，可避免明文梯度被攻击者获取而导致隐私泄露；基于安全切面，通过注入模块 11 梯度发送函数处注入第一切面程序，并通过第一切面程序对明文梯度进行拦截和加密，不需要对原有的联邦学习框架进行修改，对联邦学习业务不存在入侵性，维护成本低；通过切面服务器的可信执行环境生成加密密钥和解密密钥，保证它们不被攻击者窃取和伪造。

[86]如图 4 所示,本申请又一实施例提供一种联邦学习装置,其应用于联邦学习服务器,包括相互数据通信的注入模块 21、接收模块 22、解密模块 23 和更新模块 24。

[87]注入模块 21 设置为通过预先部署的切面底座,根据预设的第二切点和第二切面程序,在联邦学习服务器的梯度接收函数处注入第二切面程序。

[88]联邦学习服务器上预先部署有切面底座,在联邦学习开始后,注入模块 21 可通过切面底座根据第二切点和第二切面程序,在联邦学习服务器的梯度接收函数处注入第二切面程序。梯度接收函数是用于接收各联邦学习设备的待训练模型的梯度的函数,当联邦学习设备向联邦学习服务器发送梯度时,联邦学习服务器将通过梯度接收函数接收梯度。将梯度接收函数作为第二切点,并注入第二切面程序后,当联邦学习服务器通过接收梯度函数接收联邦学习设备的密文梯度时,第二切面程序会执行预设的逻辑,从而实现预设的业务。

[89]在一些实施例中,第二切点和第二切面程序可以是预先存储在联邦学习服务器中的,当联邦学习开始后,切面底座将启动,注入模块 21 通过切面底座根据预设的第二切点和第二切面程序完成切点注入。在另外一些实施例中,第二切点和第二切面程序可以由切面服务器下发,当联邦学习开始后,切面服务器将第二切点和第二切面程序下发至切面底座,注入模块 21 通过切面底座完成切点注入。

[90]接收模块 22 设置为通过梯度接收函数接收各联邦学习设备发送的待训练模型的密文梯度。

[91]在联邦学习开始后,各联邦学习设备会通过预先部署的切面底座,根据预设的第一切点和第一切面程序,在联邦学习设备的梯度发送函数处注入第一切面程序;然后各联邦学习设备会分别根据本地的训练数据对待训练模型进行训练,然后得到待训练模型的明文梯度,并通过梯度发送函数向联邦学习服务器发送明文梯度,第一切面程序将拦截明文梯度,并对明文梯度进行加密,得到密文梯度,然后各联邦学习设备将各自的密文梯度发送至联邦学习服务器,接收模块 22 将通过梯度接收函数接收各联邦学习设备的密文梯度。

[92]由于接收模块 22 接收到的是密文梯度,因此可以避免攻击者获得明文梯度而导致隐私泄露。

[93]解密模块 23 设置为通过第二切面程序拦截密文梯度,并对密文梯度进行解密,得到明文梯度。

[94]在梯度接收函数接收密文梯度时，解密模块 23 将通过第二切面程序拦截密文梯度，并对其进行解密，得到对应的明文梯度，由于第二切面程序是注入在梯度接收函数处，其并不会对原有的联邦学习框架进行修改，对联邦学习业务不存在入侵性，维护成本低。

[95]由于联邦学习设备可能有多个，因此对每个联邦学习设备的密文梯度，均需要通过第二切面程序进行拦截并解密，从而得到各联邦学习设备的明文梯度。

[96]在一些实施例中，在联邦学习前，可以先生成加密密钥和解密密钥，从而使联邦学习设备采用加密密钥对明文梯度进行加密，得到密文梯度，联邦学习服务器则采用解密密钥对密文梯度进行解密，重新得到明文梯度。在一个联邦学习任务中，加密密钥和解密密钥全局唯一。

[97]在一些实施例中，加密密钥和解密密钥可通过切面服务器的可信执行环境生成。切面服务器生成加密密钥和解密密钥后，可将加密密钥发送至各联邦学习设备，以用于对明文梯度进行加密，并将解密密钥发送至联邦学习服务器，以用于对密文梯度进行解密。在发送加密密钥和解密密钥前，各联邦学习设备和联邦学习服务器可先认证切面服务器的可信执行环境是否可信，认证通过后，再与切面服务器的可信执行环境建立可信的安全传输层协议（TLS）连接，通过 TLS 连接传输加密密钥和解密密钥，以保证在传输过程中加密密钥和解密密钥的安全性。因此，联邦学习装置还可以包括连接模块，其设置为在联邦学习前，对切面服务器的可信执行环境进行远程认证，认证通过后，与可信执行环境建立可信的 TLS 连接；然后接收通过可信执行环境生成的解密密钥。

[98]在一些实施例中，切面服务器的可信执行环境可以是基于 Intel SGX 的可信执行环境。在与其进行通信前，联邦学习服务器还需要完成对可信执行环境的远程认证，远程认证过程与联邦学习设备相同，此处不再赘述。

[99]更新模块 24 设置为根据各联邦学习设备的明文梯度更新各联邦学习设备的待训练模型的参数。

[100]得到各联邦学习设备的明文梯度后，更新模块 24 将对它们进行梯度融合，得到融合后的梯度，然后根据融合后的梯度更新各联邦学习设备的待训练模型的参数。

[101]本申请实施例的联邦学习装置，接收模块 22 接收各联邦学习设备的加密后的密文梯度，并对其进行解密，得到解密后的明文梯度，以避免明文梯度在传输过程中被攻击者获取而导致隐私泄露；基于安全切面，注入模块 21 在联邦学习服务器的梯度接收函数处注入第二切面程序，解密模块 23 通过第二切面程序对密文梯度进行拦截和解密，

不需要对原有的联邦学习框架进行修改，对联邦学习业务不存在入侵性，维护成本低；通过切面服务器的可信执行环境生成加密密钥和解密密钥，保证它们不被攻击者窃取和伪造。

[102]本申请的又一实施例提供一种可读存储介质，其上存储有计算机程序，当计算机程序在计算机中执行时，令计算机执行本申请上述实施例中的联邦学习方法的步骤。

[103]本申请又一实施例提供一种电子设备，其包括存储器和处理器，存储器中存储有可执行代码，当处理器执行可执行代码时，其执行本申请上述实施例中的联邦学习方法的步骤。

[104]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。

[105]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，在实施本申请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。

[106]本领域内的技术人员应明白，本申请的实施例可提供为方法、系统、或计算机程序产品。因此，本申请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，本申请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。

[107]本申请是参照根据本申请实施例的方法、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数据处理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数据处理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。

[108]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数据处理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。

[109]这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，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。

[110]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。

[111]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。

[112]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。

[113]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。

[114]本领域技术人员应明白，本申请的实施例可提供为方法、系统或计算机程序产品。因此，本申请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，本申请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。

[115]本申请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申请,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。

[116]本申请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。

[117]以上所述的,仅为本申请的较佳实施例,并非用以限定本申请的范围,本申请的上述实施例还可以做出各种变化。即凡是依据本申请的权利要求书及说明书内容所作的简单、等效变化与修饰,皆落入本申请的权利要求保护范围。本申请未详尽描述的均为常规技术内容。

权利要求书

1、一种联邦学习方法，所述方法应用于联邦学习设备，所述方法包括：

联邦学习设备通过预先部署的切面底座，根据预设的第一切点和第一切面程序，在所述联邦学习设备的梯度发送函数处注入所述第一切面程序；

所述联邦学习设备根据本地的训练数据对待训练模型进行训练，得到所述待训练模型的明文梯度，并通过所述梯度发送函数向联邦学习服务器发送所述明文梯度；

通过所述第一切面程序拦截所述梯度发送函数发送的明文梯度，并对所述明文梯度进行加密，得到密文梯度，将所述密文梯度发送给所述联邦学习服务器，以使所述联邦学习服务器对接收到的各联邦学习设备发送的密文梯度进行解密，并根据解密后得到的各明文梯度更新所述待训练模型的参数。

2、根据权利要求1所述的联邦学习方法，还包括：

在联邦学习前，所述联邦学习设备对切面服务器的可信执行环境进行远程认证，认证通过后，与所述可信执行环境建立可信的安全传输层协议连接；

接收通过所述可信执行环境生成的加密密钥。

3、根据权利要求1所述的联邦学习方法，所述联邦学习服务器对接收到的各联邦学习设备发送的密文梯度进行解密，具体包括：

所述联邦学习服务器通过梯度接收函数接收所述密文梯度；

通过预先注入在所述梯度接收函数处的第二切面程序拦截所述密文梯度，并对所述密文梯度进行解密。

4、一种联邦学习方法，所述方法应用于联邦学习服务器，所述方法包括：

联邦学习服务器通过预先部署的切面底座，根据预设的第二切点和第二切面程序，在所述联邦学习服务器的梯度接收函数处注入第二切面程序；

通过所述梯度接收函数接收各联邦学习设备发送的待训练模型的密文梯度；

通过所述第二切面程序拦截所述密文梯度，并对所述密文梯度进行解密，得到明文梯度；

根据各联邦学习设备的明文梯度更新各联邦学习设备的待训练模型的参数。

5、根据权利要求4所述的联邦学习方法，还包括：

在联邦学习前，对切面服务器的可信执行环境进行远程认证，认证通过后，与所述可信执行环境建立可信的安全传输层协议连接；

接收通过所述可信执行环境生成的解密密钥。

6、一种联邦学习装置，所述装置应用于联邦学习设备，所述装置包括：

注入模块, 设置为通过预先部署的切面底座, 根据预设的第一切点和第一切面程序, 在所述联邦学习设备的梯度发送函数处注入所述第一切面程序;

训练模块, 设置为根据本地的训练数据对待训练模型进行训练, 得到所述待训练模型的明文梯度, 并通过所述梯度发送函数向联邦学习服务器发送所述明文梯度;

加密模块, 设置为通过所述第一切面程序拦截所述梯度发送函数发送的明文梯度, 并对所述明文梯度进行加密, 得到密文梯度, 将所述密文梯度发送给所述联邦学习服务器, 以使所述联邦学习服务器对接收到的各联邦学习设备发送的密文梯度进行解密, 并根据解密后得到的各明文梯度更新所述待训练模型的参数。

7、根据权利要求 6 所述的联邦学习装置, 还包括连接模块, 所述连接模块设置为在联邦学习前, 所述联邦学习设备对切面服务器的可信执行环境进行远程认证, 认证通过后, 与所述可信执行环境建立可信的安全传输层协议连接; 然后接收通过所述可信执行环境生成的加密密钥。

8、根据权利要求 6 所述的联邦学习装置, 所述联邦学习服务器对接收到的各联邦学习设备发送的密文梯度进行解密, 具体包括:

所述联邦学习服务器通过梯度接收函数接收所述密文梯度;

通过预先注入在所述梯度接收函数处的第二切面程序拦截所述密文梯度, 并对所述密文梯度进行解密。

9、一种联邦学习装置, 所述装置应用于联邦学习服务器, 所述装置包括:

注入模块, 设置为通过预先部署的切面底座, 根据预设的第二切点和第二切面程序, 在所述联邦学习服务器的梯度接收函数处注入第二切面程序;

接收模块, 设置为通过所述梯度接收函数接收各联邦学习设备发送的待训练模型的密文梯度;

解密模块, 设置为通过所述第二切面程序拦截所述密文梯度, 并对所述密文梯度进行解密, 得到明文梯度;

更新模块, 设置为根据各联邦学习设备的明文梯度更新各联邦学习设备的待训练模型的参数。

10、根据权利要求 9 所述的联邦学习装置, 还包括连接模块, 所述连接模块设置为在联邦学习前, 对切面服务器的可信执行环境进行远程认证, 认证通过后, 与所述可信执行环境建立可信的安全传输层协议连接; 然后接收通过所述可信执行环境生成的解密密钥。

11、一种可读存储介质, 其上存储有计算机程序, 当计算机程序在计算机中执行时,

令计算机执行如权利要求 1-5 中任一项所述的联邦学习方法的步骤。

12、一种电子设备，其包括存储器和处理器，存储器中存储有可执行代码，当处理器执行可执行代码时，其执行如权利要求 1-5 中任一项所述的联邦学习方法的步骤。