权利要求书

1.一种基于Cybertwin的双层车联网联邦学习框架构造方法，其特征在于，在车辆设备i和中心云服务器之间部署边缘云服务器j搭建车联网双层联邦学习系统；车辆设备i，边缘云服务器j和中心云服务器协作完成模型训练；车辆设备i，边缘云服务器j，以及中心云服务器之间通过无线链路进行通信；

具体包括以下步骤：

步骤1：构建车联网双层联邦学习系统，将车联网联邦学习模型的Cybertwin网络框架分为中心云服务器、边缘云服务器j和车辆设备i三层，边缘云服务器j附着在车辆设备i预设的路测单元中；

中心云服务器用自身预设的私钥签名，将对应边缘云服务器j预设的公钥在t时刻的全局模型进行加密并发送至边缘云服务器j；

边缘云服务器j用自身预设的私钥对t时刻的加密后的全局模型进行解密，得到解密后的全局模型，保证边缘云服务器j和中心云服务器的通信安全；每个边缘云服务器j收集车辆设备i名单 ，并将全局模型发送至车辆设备i；

步骤2：车辆设备i用本地数据集训练本地模型并发送至边缘云服务器j，边缘云服务器j通过计算本地模型的贡献度分数以及通过cybertwin节点来获取车辆设备i的历史行为，将不符合预设模型要求的本地模型舍弃，得到t+1时刻的边缘云模型；所述不符合预设模型要求的本地模型为：本地模型不在预设历史行为内，或者，本地模型不在预设贡献度分数内，或者，本地模型不在预设质量内；

车辆设备i使用私钥签名，并用对应边缘云服务器j的公钥对t+1时刻的本地模型进行加密并发送至路测单元；

边缘云服务器j得到路测单元范围内的车辆设备i提交的本地模型集合{}，并将本地模型集合{}聚合得到边缘云服务器j的t+1时刻模型；

边缘云服务器j用自身的私钥签名，并通过中心云服务器公钥对边缘云服务器j的t+1时刻模型进行加密后发送至中心云服务器；

步骤3：中心云服务器将收到边缘云模型{}并进行聚合得到t+1时刻的全局模型；

步骤4：重复上述步骤1-3，直到全局迭代结束，得到最终全局模型。

2.根据权利要求1所述的方法，其特征在于，步骤2用于训练的本地数据集是由车辆设备i通过传感器、定位器等生成的；为降低回程链路的传输压力以及聚合框架的扩展性，车辆设备i只和边缘云服务器j进行通信，而边缘云服务器j既可以和车辆设备i进行通信，也可以和云服务器进行通信。

3.根据权利要求1所述的方法，其特征在于，步骤2所述车辆设备i用本地数据集训练本地模型，包括：

假设目前进行多分类任务，初始化全局模型、车辆设备i学习率η、本地训练轮次k、全局迭代轮次T；

车辆设备i收到初始化的全局模型后，通过本地数据集训练得到t+1时刻的本地模型，即；

边缘云服务器j通过下式获取车辆设备i的计算能力：





其中，表示车辆设备i​在t时刻的数据量参考值，表示车辆设备i在t+1时刻的数据量；表示本地模型在本地测试集上的模型质量表现；表示车辆设备i和边缘云服务器j测试集的JS散度。

4.根据权利要求3所述的方法，其特征在于，步骤2所述车辆设备i用本地数据集训练本地模型，之后还包括：

通过下式计算车辆设备i的全局模型质量：







其中表示滑动因子；表示车辆设备i在t+1时刻对全局模型的贡献度；表示车辆设备i在t+1时刻与全局模型的距离。

5.根据权利要求4所述的方法，其特征在于，步骤2通过下式计算车辆设备i的历史行为：



其中是一个二进制数，当为1时表示在t时刻车辆设备i的本地模型被使用，反之则为0；表示t时刻车辆设备i的本地模型质量；运算表示sigmoid函数运算。

6.根据权利要求5所述的方法，其特征在于，步骤2通过下式获取本地模型的贡献度分数：



其中，表示、差值的余弦相似度，是t+1时刻本地模型与t时刻全局模型差值，是t+1时刻本地模型与t时刻车辆设备i的差值；

如果本地模型的贡献度分数大于0，则加入聚合列表；并通过下式对本地模型的贡献度分数进行归一化得到本地模型贡献度分数的聚合权重；

。

7.根据权利要求6所述的方法，其特征在于，步骤2将本地模型集合{}聚合得到边缘云服务器j的t+1时刻模型，包括：

通过下式进行聚合并得到边缘云服务器j的t+1时刻模型：

。

8.根据权利要求7所述的方法，其特征在于，步骤3中心云服务器将收到的本地模型{}进行聚合得到t+1时刻的全局模型，包括：

中心云服务器收集边缘云服务器j的t+1时刻模型，通过下式对边缘云服务器j的t+1时刻模型进行考量并获取边缘云服务器j的t+1时刻模型的质量贡献度分数：



其中，表示边缘云服务器j的t+1时刻模型在中心云服务器测试集中的表现；

如果质量贡献度分数大于预设的质量贡献度阈值，则加入聚合列表；并通过下式对质量贡献度分数进行归一化得到RSU模型的聚合权重；



中心云服务器将收到的本地模型{}通过聚合权重进行聚合并得到t+1时刻的全局模型。

9.一种电子设备，其特征在于，所述电子设备包括处理器和存储器，所述存储器中存储有至少一条指令、至少一段程序、代码集或指令集，所述至少一条指令、所述至少一段程序、所述代码集或指令集由所述处理器加载并执行，以实现如权利要求1至7任一所述的基于Cybertwin的双层车联网联邦学习框架构造方法。

10.一种计算机可读存储介质，其特征在于，所述存储介质中存储有至少一条指令、至少一段程序、代码集或指令集，所述至少一条指令、所述至少一段程序、所述代码集或指令集由处理器加载并执行以实现如权利要求1至7任一所述的基于Cybertwin的双层车联网联邦学习框架构造方法。

说明书

**一种基于Cybertwin的双层车联网联邦学习框架构造方法**

**技术领域**

本发明涉及联邦学习技术领域，具体涉及一种基于Cybertwin的双层车联网联邦学习框架构造方法。

**背景技术**

工业是物联网应用的重要领域，随着科学技术的不断发展，车联网已然成为智能制造和工业4 .0的代名词。各类先进智能技术不断地融入到工业生产的各个环节，如人工智能(AI)、机器学习、增强/虚拟现实(AR/VR)、数字孪生/线程、云/边缘计算等智能技术。

智能车辆是未来交通领域的重要发展趋势，但要实现完全自动驾驶需要面临许多挑战，其中之一是如何获取车辆数据进行模型训练。智能车辆通过多种传感器（如摄像头、激光雷达、超声波传感器、雷达、GPS等）获取感知信息，其中摄像头每秒可能产生数兆字节的数据。直接上传所有感知数据会导致巨大的通信负载和网络资源消耗，并且存在隐私问题。因此，现有研究人员提出了一种分布式联邦学习方案，利用车联网的模型众包思想训练智能车辆的大模型。联邦学习允许多个车辆设备根据本地训练数据协作训练共享全局模型，并通过中心云服务器聚合所有本地模型参数生成改进的全局模型，以减少网络资源消耗和保护车辆设备隐私，为了实现这一目标，现有研究人员提出了基于Cybertwin网络框架的双层联邦学习聚合框架。

Cybertwin网络框架提供通信辅助、数据记录器和数字资产三个主要功能，以支持模型众包训练。通信辅助功能确保车辆在车联网环境中身份准确性，数据记录器通过分析车辆数据优化交通流量控制和道路维护策略，数字资产结合数字加密和区块链技术保障模型数据的安全性和完整性，并赋予模型数据一定的价值，这些功能为模型众包提供了理论依据和功能支持。

然而，模型众包聚合大模型存在挑战，分布式网络攻击、算力和数据结构差异、车辆高动态性、通信带宽限制和连接间断性等因素都会影响全局模型的聚合和迭代。

**发明内容**

鉴于以上所述现有技术的缺点，本发明提供基于Cybertwin的双层车联网联邦学习框架构造方法。基于Cybertwin网络框架的双层联邦学习聚合，具备扩大恶意节点容忍比例、对抗多样化后门攻击的能力，在不同车辆场景中均有效。

为实现上述效果，本发明的技术方案如下：

第一个方面，本发明提供基于Cybertwin的双层车联网联邦学习框架构造方法，在车辆设备i和中心云服务器之间部署边缘云服务器j搭建车联网双层联邦学习系统；车辆设备i，边缘云服务器j和中心云服务器协作完成模型训练；车辆设备i，边缘云服务器j，以及中心云服务器之间通过无线链路进行通信；

具体包括以下步骤：

步骤1：构建车联网双层联邦学习系统，将车联网联邦学习模型的Cybertwin网络框架分为中心云服务器、边缘云服务器j和车辆设备i三层，中心云服务器附着在预设的中心云服务器服务器中，边缘云服务器j附着在车辆设备i预设的路测单元中；

中心云服务器用自身预设的私钥签名，将对应边缘云服务器j预设的公钥在t时刻的全局模型进行加密并发送至边缘云服务器j；

边缘云服务器j用自身预设的私钥对t时刻的加密后的全局模型进行解密，得到解密后的全局模型，保证边缘云服务器j和中心云服务器的通信安全；每个边缘云服务器j收集车辆设备i名单 ，并将全局模型发送至车辆设备i；

步骤2：车辆设备i用本地数据集训练本地模型并发送至边缘云服务器j，边缘云通过计算本地模型的贡献度分数以及通过cybertwin节点来获取车辆设备i，将不符合预设模型要求的本地模型舍弃，得到t+1时刻的边缘云模型；所述不符合预设模型要求的本地模型为：本地模型不在预设历史行为内，或者，本地模型不在预设贡献度分数内，或者，本地模型不在预设质量内；

车辆设备i使用私钥签名，并用对应边缘云服务器j的公钥对t+1时刻的本地模型进行加密并发送至路测单元；

边缘云服务器j得到路测单元范围内的车辆设备i提交的本地模型集合{}，并将本地模型集合{}聚合得到边缘云服务器j的t+1时刻模型；

边缘云服务器j用自身的私钥签名，并通过中心云服务器公钥对本地模型进行加密后发送至中心云服务器；

步骤3：中心云服务器将收到的本地模型{}进行聚合得到t+1时刻的全局模型；

步骤4：重复上述步骤1-3，直到全局迭代结束，得到最终全局模型。

本发明中车辆设备i可以为车辆等物联网设备，i表示第i个车辆。本发明通过设计高效安全的聚合算法，基于Cybertwin（网络孪生）框架的双层联邦学习框架、抵御多种后门攻击。

进一步的，步骤2用于训练的本地数据集是由车辆设备i通过信息采集生成的；为降低回程链路的传输压力，车辆设备i只和边缘云服务器j进行通信，而边缘云服务器j既可以和车辆设备i进行通信，也可以和云服务器进行通信。

进一步的，步骤2所述车辆设备i用本地数据集训练本地模型，包括：

假设目前进行多分类任务，初始化全局模型、车辆设备i学习率η、本地训练轮次k、全局迭代轮次T；

车辆设备i收到初始化的全局模型后，通过本地数据集训练得到t+1时刻的本地模型，即；

边缘云服务器j通过下式获取车辆设备i的计算能力：





其中，表示车辆设备i​在t时刻的数据量参考值，表示车辆设备i​在t+1时刻的数据量；表示本地模型在本地测试集上的模型质量表现；表示车辆设备i和边缘云服务器j测试集的JS散度。

进一步的，步骤2所述车辆设备i用本地数据集训练本地模型，之后还包括：

通过下式计算车辆设备i的全局模型质量：







其中表示滑动因子；表示车辆设备i在t+1时刻对全局模型的贡献度；表示车辆设备i在t+1时刻与全局模型的距离。

进一步的，步骤2通过下式计算车辆设备i的历史行为：



其中是一个二进制数，当为1时表示在t时刻车辆设备i的本地模型被使用，反之则为0；表示t时刻车辆设备i的本地模型质量；运算表示sigmoid函数运算。

进一步的，步骤2通过下式获取本地模型的贡献度分数：



其中，表示、差值的余弦相似度，是t+1时刻本地模型与t时刻全局模型差值，是t+1时刻本地模型与t时刻车辆设备i差值；

如果本地模型的贡献度分数大于0，则加入聚合列表；并通过下式对本地模型的贡献度分数进行归一化得到本地模型贡献度分数的聚合权重；

。

进一步的，步骤2将本地模型集合{}聚合得到边缘云服务器j的t+1时刻模型，包括：

通过下式进行聚合并得到边缘云服务器j的t+1时刻模型：

。

进一步的，步骤3中心云服务器将收到的本地模型{}进行聚合得到t+1时刻的全局模型，包括：

中心云服务器收集边缘云服务器j的t+1时刻模型，通过下式对边缘云服务器j的t+1时刻模型进行考量并获取边缘云服务器j的t+1时刻模型的质量贡献度分数：



其中，表示边缘云服务器j的t+1时刻模型在中心云服务器测试集中的表现；

如果质量贡献度分数大于，则加入聚合列表；并通过下式对质量贡献度分数进行归一化得到聚合权重；



中心云服务器将收到的本地模型{}通过聚合权重进行聚合并得到t+1时刻的全局模型。

第二个方面，本发明提供一种电子设备，包括存储器和处理器，所述存储器中存储有计算机程序，所述处理器被设置为通过所述计算机程序执行基于Cybertwin的双层车联网联邦学习框架构造方法。

第三个方面，本发明提供一种计算机可读存储介质，所述计算机可读存储介质包括存储的计算机程序，其中，所述计算机程序运行时执行基于Cybertwin的双层车联网联邦学习框架构造方法。

与现有技术相比，本发明技术方案的有益效果是：

本发明针对现有鲁棒联邦学习的不足进行改进，构建车联网双层联邦学习系统，将车联网联邦学习模型的Cybertwin网络框架分为中心云服务器、边缘云服务器j和车辆设备i三层，中心云服务器附着在预设的中心云服务器服务器中，边缘云服务器j附着在车辆设备i预设的路测单元中；

车辆设备i用本地数据集训练本地模型并发送至边缘云服务器j，边缘云服务器j得到路测单元范围内的车辆设备i提交的本地模型集合{}，并将本地模型集合{}聚合得到边缘云服务器j的t+1时刻模型；中心云服务器将收到边缘云模型{}并进行聚合得到t+1时刻的全局模型；使得联邦学习场景得到扩充，适用性更强，能够抵御更多后门攻击，全局模型鲁棒性得到增强，使得恶意节点最大容错率得到了提升，适用于更多应用场景。

**附图说明**

图1是本发明基于Cybertwin网络框架的双层联邦学习框架示意图。

**具体实施方式**

以下将参照附图和优选实施例来说明本发明的实施方式，本领域技术人员可由本说明书中所揭露的内容轻易地了解本发明的其他优点与功效。本发明还可以通过另外不同的具体实施方式加以实施或应用，本说明书中的各项细节也可以基于不同观点与应用，在没有背离本发明的精神下进行各种修饰或改变。应当理解，优选实施例仅为了说明本发明，而不是为了限制本发明的保护范围。

需要说明的是，以下实施例中所提供的图示仅以示意方式说明本发明的基本构想，遂图式中仅显示与本发明中有关的组件而非按照实际实施时的组件数目、形状及尺寸绘制，其实际实施时各组件的型态、数量及比例可为一种随意的改变，且其组件布局型态也可能更为复杂。

名词释义：

RSU，是Road Side Unit的英文缩写，直译就是路侧单元的意思，是ETC系统中，安装在路侧，采用DSRC（Dedicated Short Range Communication）技术，与车载单元（OBU，On Board Unit）进行通讯，实现车辆身份识别，电子扣分的装置。在高速公路、车场管理中，在路侧安装RSU，建立无人值守的快速专用车道。

实施例

本实施例提出了一种基于Cybertwin的双层车联网联邦学习框架构造方法。请参阅图1，在车辆设备i和中心云服务器之间部署边缘云服务器j搭建车联网双层联邦学习系统；车辆设备i，边缘云服务器j和中心云服务器协作完成模型训练；车辆设备i，边缘云服务器j，以及中心云服务器之间通过无线链路进行通信；

具体包括以下步骤：

步骤1：构建车联网双层联邦学习系统，将车联网联邦学习模型的Cybertwin网络框架分为中心云服务器、边缘云服务器j和车辆设备i三层，中心云服务器附着在预设的中心云服务器服务器中，边缘云服务器j附着在车辆设备i预设的路测单元中；

中心云服务器用自身预设的私钥签名，将对应边缘云服务器j预设的公钥在t时刻的全局模型进行加密并发送至边缘云服务器j；

边缘云服务器j用自身预设的私钥对t时刻的加密后的全局模型进行解密，得到解密后的全局模型，以此来保证边缘云服务器j和中心云服务器的通信安全；每个边缘云服务器j收集车辆设备i名单 ，并将全局模型发送至车辆设备i；

步骤2：车辆设备i用本地数据集训练本地模型并发送至边缘云服务器j，边缘云通过计算本地模型的贡献度分数以及通过cybertwin节点来获取车辆设备i，将不符合预设模型要求的本地模型舍弃，得到t+1时刻的边缘云模型；所述不符合预设模型要求的本地模型为：本地模型不在预设历史行为内，或者，本地模型不在预设贡献度分数内，或者，本地模型不在预设质量内；

在h时刻内，车辆设备i使用私钥签名，并用对应边缘云服务器j的公钥对t+1时刻的本地模型进行加密并发送至路测单元；

边缘云服务器j得到路测单元范围内的车辆设备i提交的本地模型集合{}，并将本地模型集合{}聚合得到边缘云服务器j的t+1时刻模型；

边缘云服务器j用自身的私钥签名，并通过中心云服务器公钥对本地模型进行加密后发送至中心云服务器；

步骤3：中心云服务器将收到的本地模型{}进行聚合得到t+1时刻的全局模型；

步骤4：重复上述步骤1-3，直到全局迭代结束，得到最终全局模型。

作为优选的技术方案，本实施例中，步骤2用于训练的本地数据集是由车辆设备i通过信息采集生成的；为降低回程链路的传输压力，车辆设备i只和边缘云服务器j进行通信，而边缘云服务器j既可以和车辆设备i进行通信，也可以和云服务器进行通信。

作为优选的技术方案，本实施例中，步骤2所述车辆设备i用本地数据集训练本地模型，包括：

假设目前进行多分类任务，初始化全局模型、车辆设备i学习率η、本地训练轮次k（实际应用时可以根据车辆设备i情况调整来得到更好的效果）、全局迭代轮次T；

车辆设备i收到初始化的全局模型后，通过本地数据集训练得到t+1时刻的本地模型，即；

以边缘云服务器j举例，得到{}后开始计算其的贡献度和历史行为；

边缘云服务器j通过下式获取车辆设备i的计算能力：





其中，表示车辆设备i​在t时刻的数据量参考值，具体取值根据不同的任务而定；表示车辆设备i​在t+1时刻的数据量；表示本地模型在本地测试集上的模型质量表现；表示车辆设备i和边缘云服务器j测试集的JS散度。

可以理解的是，数据量指车辆设备i所拥有的数据集大小，比如就多分类图像识别来说，假设车辆设备iA有3000张，车辆设备iB有2000张...是比较常见的数据分布形式。本地模型在训练时将数据集分为训练集和测试集，本地测试集即训练所用的测试集。

作为优选的技术方案，本实施例中，步骤2所述车辆设备i用本地数据集训练本地模型，之后还包括：

通过下式计算车辆设备i的全局模型质量：







其中表示滑动因子；表示车辆设备i在t+1时刻对全局模型的贡献度；表示车辆设备i在t+1时刻与全局模型的距离。

作为优选的技术方案，本实施例中，步骤2通过下式计算车辆设备i的历史行为：



其中是一个二进制数，当为1时表示在t时刻车辆设备i的本地模型被使用，反之则为0；表示t时刻车辆设备i的本地模型质量；运算表示sigmoid函数运算，使得更靠近当前时刻的事件更有参考意义。

作为优选的技术方案，本实施例中，步骤2通过下式获取本地模型的贡献度分数：



其中，表示、差值的余弦相似度，是t+1时刻本地模型与t时刻全局模型差值，是t+1时刻本地模型与t时刻车辆设备i差值；

如果本地模型的贡献度分数大于0，则加入聚合列表；并通过下式对本地模型的贡献度分数进行归一化得到本地模型贡献度分数的聚合权重；

。

作为优选的技术方案，本实施例中，步骤2将本地模型集合{}聚合得到边缘云服务器j的t+1时刻模型，包括：

通过下式进行聚合并得到边缘云服务器j的t+1时刻模型：

。

作为优选的技术方案，本实施例中，步骤3中心云服务器将收到的本地模型{}进行聚合得到t+1时刻的全局模型，包括：

中心云服务器收集边缘云服务器j的t+1时刻模型，通过下式对边缘云服务器j的t+1时刻模型进行考量并获取边缘云服务器j的t+1时刻模型的质量贡献度分数：



其中，表示边缘云服务器j的t+1时刻模型在中心云服务器测试集中的表现，为的是即使某一个边缘云服务器j出现问题，在中心云服务器这里也能识别出来；

如果质量贡献度分数大于，则加入聚合列表；并通过下式对质量贡献度分数进行归一化得到聚合权重；



中心云服务器将收到的本地模型{}通过聚合权重进行聚合并得到t+1时刻的全局模型。

需要说明的是，本发明中车辆设备i可以为车辆等物联网设备。

在本发明的另一个实施例中，还提供了一种电子设备，包括：一个或多个处理器；存储装置，用于存储一个或多个程序，当所述一个或多个程序被所述一个或多个处理器执行时，使得本发明实现如上任一实施例中所述方法。

在本实施例中，适用于来实现本发明实施例的电子设备的计算机系统包括中央处理单元(CentralProcessingUnit，CPU)，其可以根据存储在只读存储器(Read‑OnlyMemory，ROM)中的程序或者从储存部分加载到随机访问存储器(RandomAccessMemory，RAM)中的程序而执行各种适当的动作和处理，例如执行上述实施例中所述的方法。在RAM中，还存储有系统操作所需的各种程序和数据。CPU、ROM以及RAM通过总线彼此相连。输入/输出(Input/Output，I/O)接口也连接至总线。

以下部件连接至I/O接口：包括键盘、鼠标等的输入部分；包括诸如阴极射线管(CathodeRayTube，CRT)、液晶显示器(LiquidCrystalDisplay，LCD)等以及扬声器等的输出部分；包括硬盘等的储存部分；以及包括诸如LAN(LocalAreaNetwork，局域网)卡、调制解调器等的网络接口卡的通信部分。通信部分经由诸如因特网的网络执行通信处理。驱动器也根据需要连接至I/O接口。可拆卸介质，诸如磁盘、光盘、磁光盘、半导体存储器等等，根据需要安装在驱动器上，以便于从其上读出的计算机程序根据需要被安装入储存部分。

特别地，根据本发明的实施例，上文参考流程图描述的过程可以被实现为计算机软件程序。例如，本发明的实施例包括一种计算机程序产品，其包括承载在计算机可读介质上的计算机程序，该计算机程序包含用于执行流程图所示的方法的计算机程序。在这样的实施例中，该计算机程序可以通过通信部分从网络上被下载和安装，和/或从可拆卸介质被安装。在该计算机程序被中央处理单元(CPU)执行时，执行本发明的系统中限定的各种功能。

应当注意，尽管在上文详细描述中提及了用于动作执行的设备的若干模块或者单元，但是这种划分并非强制性的。实际上，根据本发明的实施方式，上文描述的两个或更多模块或者单元的特征和功能可以在一个模块或者单元中具体化。反之，上文描述的一个模块或者单元的特征和功能可以进一步划分为由多个模块或者单元来具体化。

在本实施例中，本发明还提供了一种计算机可读存储介质，其上存储有计算机程序，当所述计算机程序被计算机的处理器执行时，使计算机执行如前述任一实施例提供的所述方法。该计算机可读存储介质可以是上述实施例中描述的电子设备中所包含的，也可以是单独存在，而未装配入该电子设备中。

通过以上的实施方式的描述，本领域的技术人员易于理解，描述的示例实施方式可以通过软件实现，也可以通过软件结合必要的硬件的方式来实现。因此，根据本发明实施方式的技术方案可以以软件产品的形式体现出来，该软件产品可以存储在一个非易失性存储介质(可以是CD‑ROM，U盘，移动硬盘等)中或网络上，包括若干指令以使得一台计算设备(可以是个人计算机、服务器、触控终端、或者网络设备等)执行根据本发明实施方式的方法。

实施本发明实施例，具有如下有益效果：

1）本发明创造所要解决的技术问题：

在车联网中，通信复杂性、数据结构的不同以及多种后门攻击无形增加了模型聚合的难度。因此需要设计新的联邦学习框架来扩大恶意节点容忍比例，设计新联邦学习方法来增强模型对多种后门攻击稳定性，同时还需要保证模型在复杂通信中的鲁棒性。

2）解决其技术问题采用的技术方案

本发明综合考虑了车联网领域中多个关键因素，用于解决智能车辆设备i数据获取和模型训练中存在的多种后门攻击等复杂性挑战。本发明中，为了实现本地模型聚合过程的优化，在考虑模型之间距离和车辆设备i数据异构程度的基础上，将本地模型集合{}聚合得到边缘云服务器j的t+1时刻模型。本发明能够合理地反映各个本地模型的性能和数据质量，从而确保每个本地模型的贡献得到准确评估和有效利用。同时，还通过考虑车辆设备i对全局模型的贡献，实现了动态调整参与训练的车辆设备i数量和权重的能力，能够最大程度地利用有贡献的设备，提升全局模型的性能。针对车辆设备i通信的复杂性，采用了本发明的联邦学习框架，以降低通信复杂性所带来的不可靠，并提高最大恶意容忍节点比例。Cybertwin网络框架充分考虑了在车联网中应用Cybertwin网络框架，从而有效增强车联网联邦学习模型的适用性和鲁棒性。

显然，本发明的上述实施例仅仅是为清楚地说明本发明所作的举例，而并非是对本发明的实施方式的限定。对于所属领域的普通技术人员来说，在上述说明的基础上还可以做出其它不同形式的变化或变动。这里无需也无法对所有的实施方式予以穷举。凡在本发明的精神和原则之内所作的任何修改、等同替换和改进等，均应包含在本发明权利要求的保护范围之内。