(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 112653752 A
(43)申请公布日 2021.04.13

(21)申请号 202011505923.4

(22)申请日 2020.12.18

(71)申请人 重庆大学
地址 400044 重庆市沙坪坝区沙坪坝正街174号
申请人 重庆工业大数据创新中心有限公司

(72)发明人 欧阳飞 叶春晓 张亚兵 邢镔

(74)专利代理机构 北京同恒源知识产权代理有限公司 11275
代理人 赵荣之

(51)Int.Cl.
H04L 29/08(2006.01)
H04L 12/24(2006.01)
H04L 29/06(2006.01)
H04L 9/08(2006.01)
H04W 4/38(2018.01)

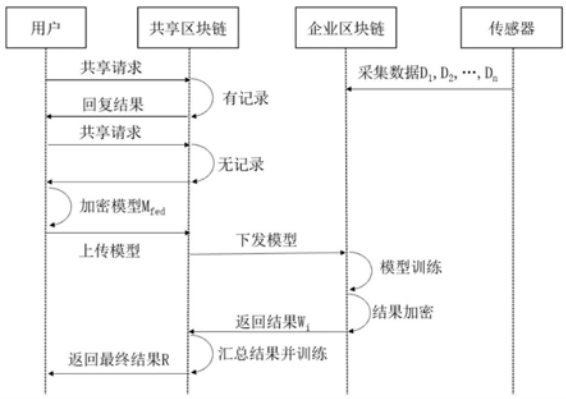
权利要求书2页 说明书7页 附图1页

(54)发明名称

基于联邦学习的区块链工业物联网数据共享方法

(57)摘要

本发明涉及一种基于联邦学习的区块链工业物联网数据共享方法，属于工业物联网技术领域。该方法将各物联网终端设备采集到的数据通过网络传输到本地区块链上，需要共享的数据在本地区块链进行训练无损学习模型，将结果传递参数到共享区块链，共享区块链上存储相同训练模型并对传入结果进行整合计算，最后将结果反馈给用户使用。本发明保证了隐私数据不被泄露，企业可以根据需求选择参与运算的区块以及数据，节约运算性能。在数据共享传输的过程中，只传输运算结果和模型参数密文，采用同态加密传输机制，保障传输的安全性。



CN 112653752 A

1.一种基于联邦学习的区块链工业物联网数据共享方法,其特征在于,将各物联网终端设备采集到的数据通过网络传输到本地区块链上,需要共享的数据在本地区块链进行训练无损学习模型,将结果传递参数到共享区块链,共享区块链上存储相同训练模型并对传入结果进行整合计算,最后将结果反馈给用户使用;具体包括以下步骤:

S1:数据准备阶段;

S2:密钥生成阶段;

S3:数据加密与传输;

S4:数据解密阶段;

S5:数据共享阶段。

2.根据权利要求1所述的区块链工业物联网数据共享方法,其特征在于,步骤S1中,数据准备阶段具体包括:

S11:n个不同的传感器收集到的数据分别定义为D_1,D_2,D_3,…,D_n,分别存放在区块B_1,B_2,B_3,…,B_n上;每个企业都有各自的区块链,分别存放各自的数据;

S12:传感器采集到的数据D_1,D_2,D_3,…,D_n,根据保密等级不同及数据量大小放入不同的企业区块上;共享数据的时候,企业用户根据实际需求及保密等级选择共享数据D_i;

S13:当数据D_i能共享时,该数据所在区块链会从共享区块链下载训练模型M_{fed},并生成新的区块B_i,然后对数据D_i进行训练计算,得到训练结果$W_i=M_{fed}(D_i)$;不同的企业根据能共享的数据区块,分别训练得到不同的结果w_1,w_2,w_3,…,w_n;

S14:若需要共享的数据刚好是传感器刚刚采集到的数据,使用异步传输机制,即每隔固定时间t训练一次模型,得到训练结果w_k;对于采集传输时间大于时间t的数据,采取放弃。

3.根据权利要求2所述的区块链工业物联网数据共享方法,其特征在于,步骤S2中,密钥生成阶段具体包括:

S21:需要共享的区块B_i运行密钥生成函数KeyGen,产生加密数据$E(w_i)$所用的密钥Key;

S22:选择两个独立的大素数p,q,即满足gcd(pq,(p-1)(q-1))=1,以保证这两个素数的长度相等;

S23:计算n=pq,λ=lcm,(p-1)(q-1);随机选择一个整数g,$g \in Z_{n^2}^*$;μ=$(L(g^{\lambda} \bmod n^2))^{-1}$,这里L被定义为$L(x)=\frac{x-1}{n}$,其中公钥为(n,g),私钥为(λ,μ);

S24:如果使用等效长度的p,q,则设置上述密钥生成步骤的更简单的变体g=n+1,lambda=ψ(n);

mμ=$\psi(n)^{-1} \bmod n$,这里ψ(n)=(p-1)(q-1);

S25:同理,在共享区块链上也需要生成模型传输用的公钥和私钥。

4.根据权利要求3所述的区块链工业物联网数据共享方法,其特征在于,步骤S3中,数据加密与传输具体包括:企业区块链训练后的结果w_i和训练模型M_{fed}是需要加密的密文,在这里,$0 \leqslant w_i < n$,$0 \leqslant M_{fed} < n$;具体过程如下:

S31:随机选择一个整数r,0<r<n,$r \in Z_{n^2}^*$;与n互质,即gcd(r,n)=1;区块B_i计算密文$c_{w_i}=E(w_i,r)=g^{w_i} \cdot r^n \bmod n^2$;

S32:将密文c_{w_i}和$c_{M_{fed}}$发送给共享区块链上的区块BS_i,BS_1,BS_2,…,BS_n表示由各个企业共享区块链训练以后传入共享区块链的数据,对应于训练结果w_1,w_2,w_3,…,w_n;

S33:共享区块链上同样计算好模型的密文$c_{M_{fed}} = E(M_{fed}, r) = g^{M_{fed}} \cdot r^n \bmod n^2$,当企业需要共享数据前需要下载训练模型$M_{fed}$,即下载加密后的密文$c_{M_{fed}}$;

S34:当用户上传新的训练模型的时候,共享区块链需要重新计算训练模型密文$c_{M_{fed}}$为企业区块链提供新的密文下载。

5.根据权利要求4所述的区块链工业物联网数据共享方法,其特征在于,步骤S4中,数据解密阶段具体包括:

S41:共享区块链上的区块BS_i接收到传入的数据c_{w_i}后,对接收到的数据进行解密处理,$c_{w_i} \in Z_{n^2}^*$,计算出明文$m_i = D(c_{w_i}) = L(c_{w_i}^{\lambda} \bmod n^2) \cdot \mu \bmod n$;

S42:汇总当前所有区块的数据$M=\{m_1, m_2, m_3, \cdots, m_n\}$,M是各个区块的训练结果$w_1$,$w_2$,$w_3$,…,$w_n$的集合;

S43:同理,当需要共享数据的区块B_i下载了训练模型密文$c_{M_{fed}}$后,也是通过该方法进行解密。

6.根据权利要求5所述的区块链工业物联网数据共享方法,其特征在于,步骤S5中,数据共享阶段具体包括:共享区块链汇聚完当前所有数据M后,开始运行对应训练模型计算最终结果$R=M_{fed}(M)$,并将结果保存到新的区块,并将结果提供给用户查询使用。

7.根据权利要求1所述的区块链工业物联网数据共享方法,其特征在于,数据传输和接收时仅提供数据使用权的接口。

基于联邦学习的区块链工业物联网数据共享方法

技术领域

[0001] 本发明属于工业物联网技术领域，涉及密码学、区块链技术、信息安全、工业物联网技术领域，具体涉及一种基于联邦学习的区块链工业物联网数据共享方法。

背景技术

[0002] 工业物联网数据共享一直是人们关心的热点话题之一。工业物联网设备众多，各企业独立存储和维护各自数据，常出现数据孤岛；设备之间每时每刻都产生着海量的数据；隐私数据泄露等安全性问题经常出现。区块链具有去中心化、透明可信、强安全的共识机制特性，越来越多企业选择将工业物联网数据放在区块链上，在内部实现数据共享。当数据需要跨企业共享时，信任就成了最大的问题，人们并不希望把数据直接共享出去，因为数据之间可能含有部分敏感数据，而直接“脱敏”会影响数据的计算结果准确度，同时也担心在传输的过程中因为窃听等原因造成数据泄露。这些都让跨企业数据共享和跨企业大数据科学研究之路变得更加艰难。

[0003] 联邦学习是一种新兴的人工智能基础技术，其设计目标是在保障大数据共享交换时的信息安全、保护终端个人数据隐私、保证合法合规的前提下，在多参与者或多计算节点之间开展高效率的机器学习，有望成为下一代人工智能协同算法和协作网络的基础。因其强大的隐私保护能力和打破“数据孤岛”的能力，能很好的解决上述问题。

发明内容

[0004] 有鉴于此，本发明的目的在于提供一种基于联邦学习的区块链工业物联网数据共享方法，保证区块链中保持的隐私数据不被泄露，企业可以根据需求选择参与运算的区块以及数据，节约运算性能。

[0005] 为达到上述目的，本发明提供如下技术方案：

[0006] 一种基于联邦学习的区块链工业物联网数据共享方法，将各物联网终端设备采集到的数据通过网络传输到本地区块链上，需要共享的数据在本地区块链进行训练无损学习模型，将结果传递参数到共享区块链，共享区块链上存储相同训练模型并对传入结果进行整合计算，最后将结果反馈给用户使用；具体包括以下步骤：

[0007] S1：数据准备阶段；

[0008] S2：密钥生成阶段；

[0009] S3：数据加密与传输；

[0010] S4：数据解密阶段；

[0011] S5：数据共享阶段。

[0012] 进一步，步骤S1中，数据准备阶段具体包括：

[0013] S11：n个不同的传感器收集到的数据分别定义为$D_1,D_2,D_3,\cdots,D_n$，分别存放在区块$B_1,B_2,B_3,\cdots,B_n$上；每个企业都有各自的区块链，分别存放各自的数据；

[0014] S12：传感器采集到的数据$D_1,D_2,D_3,\cdots,D_n$，根据保密等级不同及数据量大小放入

不同的企业区块上;共享数据的时候,企业用户可以根据实际需求及保密等级选择共享数据D_i;

[0015] S13:当数据D_i能共享时,该数据所在区块链会从共享区块链下载训练模型M_{fed},并生成新的区块B_i,然后对数据D_i进行训练计算,得到训练结果$W_i=M_{fed}(D_i)$;不同的企业根据能共享的数据区块,分别训练得到不同的结果$w_1,w_2,w_3,\cdots,w_n$;此处因为各个传感器的性能不一致,导致传输到企业区块上的数据时间也不一致。

[0016] S14:若需要共享的数据刚好是传感器刚刚采集到的数据,可以使用异步传输机制,即每隔固定时间t训练一次模型,得到训练结果w_k;对于采集传输时间大于时间t的数据,可以适当采取放弃。

[0017] 进一步,步骤S2中,密钥生成阶段具体包括:

[0018] S21:需要共享的区块B_i运行密钥生成函数KeyGen,产生加密数据$E(w_i)$所用的密钥Key;

[0019] S22:选择两个独立的大素数p,q,即满足$\gcd(pq,(p-1)(q-1))=1$,以保证这两个素数的长度相等;

[0020] S23:计算$n=pq,\lambda=\mathrm{lcm},(p-1)(q-1)$;随机选择一个整数g,$g\in Z_{n^2}^*$;$\mu=(L(g^{\lambda}\bmod n^2))^{-1}$,这里L被定义为$L(x)=\frac{x-1}{n}$,其中公钥为(n,g),私钥为$(\lambda,\mu)$;

[0021] S24:如果使用等效长度的p,q,则可以设置上述密钥生成步骤的更简单的变体$g=n+1,\mathrm{lambda}=\psi(n)$;

[0022] $m\mu=\psi(n)^{-1}\bmod n$,这里$\psi(n)=(p-1)(q-1)$;

[0023] S25:同理,在共享区块链上也需要生成模型传输用的公钥和私钥。

[0024] 进一步,步骤S3中,数据加密与传输具体包括:企业区块链训练后的结果w_i和训练模型M_{fed}是需要加密的密文,在这里,$0\leqslant w_i<n,0\leqslant M_{fed}<n$;具体过程如下:

[0025] S31:随机选择一个整数r,$0<r<n$,$r\in Z_{n^2}^*$;与n互质,即$\gcd(r,n)=1$;区块B_i计算密文$c_{w_i}=E(w_i,r)=g^{w_i}\cdot r^n \bmod n^2$;

[0026] S32:将密文c_{w_i}和$c_{M_{fed}}$发送给共享区块链上的区块BS_i,$BS_1,BS_2,\cdots,BS_n$表示由各个企业共享区块链训练以后传入共享区块链的数据,对应于训练结果$w_1,w_2,w_3,\cdots,w_n$;

[0027] S33:共享区块链上同样计算好模型的密文$c_{M_{fed}}=E(M_{fed},r)=g^{M_{fed}}\cdot r^n \bmod n^2$,当企业需要共享数据前需要下载训练模型$M_{fed}$,即下载加密后的密文$c_{M_{fed}}$;

[0028] S34:当用户上传新的训练模型的时候,共享区块链需要重新计算训练模型密文$c_{M_{fed}}$为企业区块链提供新的密文下载。因为区块链不可篡改的特点,新上传的模型密文不会覆盖旧的模型密文。

[0029] 进一步,步骤S4中,数据解密阶段具体包括:

[0030] S41:共享区块链上的区块BS_i接收到传入的数据c_{w_i}后,对接收到的数据进行解密处理,$c_{w_i}\in Z_{n^2}^*$,计算出明文$m_i=D(c_{w_i})=L(c_{w_i}^{\lambda} \bmod n^2)\cdot\mu \bmod n$;

[0031] 证明：$m_i = L\left(c_{w_i}^{\lambda} \bmod n^2\right) \cdot \mu \bmod n = \frac{L(c_{w_i}^{\lambda} \bmod n^2)}{L(g^{\lambda} \bmod n^2)} \bmod n$；

[0032] 引入私钥λ，根据Carmichael定理得：

[0033] $c_{w_i}^{\lambda} = (g^{m_i} \cdot r^n)^{\lambda} = g^{m_i\lambda} \cdot r^{n\lambda} = g^{m_i\lambda}$.

[0034] 根据关系$(1+n)^x \equiv 1+nx \bmod n^2$得：

[0035] $g^{m_i\lambda} = ((1+n)^{\alpha}\beta^n)^{\lambda m_i} = (1+n)^{\alpha\lambda m_i}\beta^{n\lambda m_i} \equiv (1+\alpha\lambda m_i n) mod\ n^2$；

[0036] 使用L(x)函数得：$\frac{L(c_{w_i}^{\lambda} \bmod n^2)}{L(g^{\lambda} \bmod n^2)} \bmod n = \frac{L(1+\alpha\lambda m_i n)}{L(1+\alpha\lambda n)} \bmod n = \frac{\alpha\lambda m_i n}{\alpha\lambda n} \bmod n = m_i$；

[0037] S42：汇总当前所有区块的数据$M=\{m_1, m_2, m_3, \cdots, m_n\}$，M是各个区块的训练结果$w_1, w_2, w_3, \cdots, w_n$的集合；

[0038] S43：同理，当需要共享数据的区块B_i下载了训练模型密文$C_{M_{fed}}$后，也是通过该方法进行解密。

[0039] 进一步，步骤S5中，数据共享阶段具体包括：共享区块链汇聚完当前所有数据M后，开始运行对应训练模型计算最终结果R＝M_fed(M)，并将结果保存到新的区块，并将结果提供给用户查询使用。模型可以根据需求定期运行或者手动运行，每次运行重复解密和计算两部分即可。当然，因为区块链的不可以篡改特点，模型每次运行结果都将保存。用户可以选择直接下载以前的数据，也可以重新运行产生最新的数据。同时，用户也可以根据实际需求选择用以前的模型进行计算或选择上传新的模型。根据数据量的大小不同，每次运行时间会有所差别，用户也可以有选择的选择部分企业的工业物联网数据进行运算，对于延迟比较大的数据结果可以选择性运行。

[0040] 进一步，数据传输和接收时仅提供数据使用权的接口。

[0041] 本发明的有益效果在于：与现有的技术相比，本发明提供了一种新颖的工业物联网数据共享机制，将工业物联网设备采集到的数据均保存在本地区块链中，保证了隐私数据不被泄露，企业可以根据需求选择参与运算的区块以及数据，节约运算性能。在数据共享传输的过程中，只传输运算结果和模型参数密文，采用同态加密传输机制，保障传输的安全性。

[0042] 本发明的其他优点、目标和特征在某种程度上将在随后的说明书中进行阐述，并且在某种程度上，基于对下文的考察研究对本领域技术人员而言将是显而易见的，或者可以从本发明的实践中得到教导。本发明的目标和其他优点可以通过下面的说明书来实现和获得。

附图说明

[0043] 为了使本发明的目的、技术方案和优点更加清楚，下面将结合附图对本发明作优选的详细描述，其中：

[0044] 图1为本发明基于联邦学习的区块链工业物联网数据共享方法的流程图；

[0045] 图2为本发明基于联邦学习的区块链工业物联网数据共享模型应用案例图。

具体实施方式

[0046] 以下通过特定的具体实例说明本发明的实施方式，本领域技术人员可由本说明书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。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，在不冲突的情况下，以下实施例及实施例中的特征可以相互组合。

[0047] 请参阅图1～图2，本发明提供一种适用于基于区块链构建的工业物联网环境中的基于联邦学习的区块链工业物联网数据共享方法，包括下列步骤：

[0048] 1)数据准备阶段

[0049] (1)n个不同的传感器收集到的数据分别定义为$D_1,D_2,D_3,\cdots,D_n$，分别存放在区块$B_1,B_2,B_3,\cdots,B_n$上。每个企业都有各自的区块链，分别存放各自的数据。

[0050] (2)传感器采集到的数据$D_1,D_2,D_3,\cdots,D_n$，根据保密等级不同及数据量大小放入不同的企业区块上。共享数据的时候，企业用户可以根据实际需求及保密等级选择共享数据D_i。

[0051] (3)当数据D_i可以共享时，该区块链会从共享区块链下载训练模型M_{fed}，并生成新的区块B_i，然后对数据D_i进行训练计算，得到训练结果$W_i=M_{fed}(D_i)$。不同的企业根据可以共享的数据区块，分别训练得到不同的结果$w_1,w_2,w_3,\cdots,w_n$.此处因为各个传感器的性能不一致，导致传输到企业区块上的数据时间也不一致。

[0052] (4)若需要共享的数据刚好是传感器刚刚采集到的数据，可以使用异步传输机制。即每隔固定时间t训练一次模型，得到训练结果w_k。对于采集传输时间大于时间t的数据，可以适当采取放弃。

[0053] 2)密钥生成阶段

[0054] (1)需要共享的区块B_i运行密钥生成函数KeyGen，产生加密数据$E(w_i)$所用的密钥Key。

[0055] (2)选择两个独立的大素数p,q，即满足$\gcd(pq,(p-1)(q-1))=1$，以保证这两个素数的长度相等。

[0056] (3)计算$n=pq,\lambda=1cm,(p-1)(q-1)$.随机选择一个整数g，$g\in Z_{n^2}^*$.$\mu=(L(g^{\lambda}\bmod n^2))^{-1}$，这里L被定义为$L(x)=\frac{x-1}{n}$.其中公钥为(n,g)，私钥为$(\lambda,\mu)$。

[0057] (4)如果使用等效长度的p,q，则可以设置上述密钥生成步骤的更简单的变体$g=n+1,lambda=\psi(n)$.

[0058] $m\mu=\psi(n)^{-1}\bmod n$.这里$\psi(n)=(p-1)(q-1)$.

[0059] (5)同理，在共享区块链上也需要生成模型传输用的公钥和私钥。

[0060] 3)数据加密与传输

[0061] 联邦学习在一定的程度上保护了本地用户数据集的隐私安全问题，但在真正使用中，并非绝对安全，仍然会存在隐私泄露风险。最常见的两种攻击是模型提取攻击和模型逆向攻击。攻击者通过模型提取和分析，窃取模型参数和本地用户上传的参数，破坏模型保密性，对整个模型的运算结果造成很大的影响。故在本方案中，我们引入同态加密作为模型及

参数的加密传输。

[0062] 企业区块链训练后的结果w_i和训练模型M_{fed}是我们需要加密的密文,在这里,$0 \leqslant w_i < n$,$0 \leqslant M_{fed} < n$.具体过程如下:

[0063] (1)随机选择一个整数r,$0<r<n$,$r \in Z_{n^2}^*$.与n互质,即gcd(r,n)=1.区块B_i计算密文$c_{w_i} = E(w_i, r) = g^{w_i} \cdot r^n \bmod n^2$.

[0064] (2)将密文c_{w_i}和$c_{M_{fed}}$发送给共享区块链上的区块BS_i.BS_1,BS_2,…,BS_n表示由各个企业共享区块链训练以后传入共享区块链的数据,对应于训练结果w_1,w_2,w_3,…,w_n.

[0065] (3)共享区块链上同样计算好模型的密文

$c_{M_{fed}} = E(M_{fed}, r) = g^{M_{fed}} \cdot r^n \bmod n^2$,当企业需要共享数据前需要下载训练模型$M_{fed}$,即下载加密后的密文$c_{M_{fed}}$.

[0066] (4)当用户上传新的训练模型的时候,共享区块链需要重新计算训练模型密文$c_{M_{fed}}$为企业区块链提供新的密文下载。因为区块链不可篡改的特点,新上传的模型密文不会覆盖旧的模型密文。

[0067] 4)数据解密阶段

[0068] (1)共享区块链上的区块BS_i接收到传入的数据c_{w_i}后,对接收到的数据进行解密处理,$c_{w_i} \in Z_{n^2}^*$,计算出明文$m_i = D(c_{w_i}) = L(c_{w_i}^{\lambda} \bmod n^2) \cdot \mu \bmod n$.

[0069] 证明:$m_i = L(c_{w_i}^{\lambda} \bmod n^2) \cdot \mu \bmod n = \frac{L(c_{w_i}^{\lambda} \bmod n^2)}{L(g^{\lambda} \bmod n^2)} \bmod n$.

[0070] 引入私钥λ,根据Carmichael定理得:

[0071] $c_{w_i}^{\lambda} = (g^{m_i} \cdot r^n)^{\lambda} = g^{m_i \lambda} \cdot r^{n\lambda} = g^{m_i \lambda}$.

[0072] 根据关系$(1+n)^x \equiv 1+nx \bmod n^2$得:

[0073] $g^{m_i \lambda} = ((1+n)^{\alpha} \beta^n)^{\lambda m_i} = (1+n)^{\alpha \lambda m_i} \beta^{n \lambda m_i} \equiv (1+\alpha \lambda m_i n) \bmod n^2$.

[0074] 使用L(x)函数得:$\frac{L(c_{w_i}^{\lambda} \bmod n^2)}{L(g^{\lambda} \bmod n^2)} \bmod n = \frac{L(1+\alpha \lambda m_i n)}{L(1+\alpha \lambda n)} \bmod n = \frac{\alpha \lambda m_i n}{\alpha \lambda n} \bmod n = m_i$.

[0075] (2)汇总当前所有区块的数据M={m_1,m_2,m_3,…,m_n},M就是之前各个区块的训练结果w_1,w_2,w_3,…,w_n的集合。

[0076] (3)同理,当需要共享数据的区块B_i下载了训练模型密文$c_{M_{fed}}$后,也是通过该方法进行解密。

[0077] 5)数据共享阶段

[0078] 共享区块链汇聚完当前所有数据M后,开始运行对应训练模型计算最终结果R=M_{fed}(M),并将结果保存到新的区块.并将结果提供给用户查询使用。模型可以根据需求定期运行或者手动运行,每次运行重复解密和计算两部分即可。当然,因为区块链的不可以篡改特点,模型每次运行结果都将保存。用户可以选择直接下载以前的数据,也可以重新运行产生最新的数据。同时,用户也可以根据实际需求选择用以前的模型进行计算或选择上传新的模型。根据数据量的大小不同,每次运行时间会有所差别,用户也可以有选择的选择部分企业的工业物联网数据进行运算,对于延迟比较大的数据结果可以选择性运行。具体过程

如下所示：

Algorithm 1. Sharing model based on Federated Learning and blockchain

Input: data $D_1, D_2, D_3, \ldots, D_n$
Output: data training result R

begin
  if M_{fed} exists **then**
    return $R = M_{fed}(M)$;
  end
  if M_{fed} NOT exists **then**
    User **encrypts** model M_{fed} to $c_{M_{fed}}$
    User **uploads** $c_{M_{fed}}$ to Shared blockchain;
    The Shared blockchain **sends** the $c_{M_{fed}}$ to the enterprise blockchain
    enterprise blockchain **decrypts** $c_{M_{fed}}$ to M_{fed}
      enterprise blockchain **generate** $W_i = M_{fed}(D_i)$
      enterprise blockchain **encrypts** W_i to c_{w_i}
    enterprise blockchain **send** c_{w_i} to Shared blockchain
    Shared blockchain **decrypts** c_{w_i} to W_i
    Shared blockchain **computes** $W = \sum_{i=1}^{n} w_i$
    Shared blockchain **computes** $R = M_{fed}(W)$
    return $R = M_{fed}(M)$;
    end if
end

[0079]

[0080] 步骤1)和5)中数据传输和接收时仅提供数据使用权的接口。

[0081] 实施例1：本实施例是基于混合现实和全息投影的智能化设备视频显示机制，如图2所示，具体包括以下步骤：

[0082] 1)数据采集阶段。不同的企业A、B、C拥有不同的数据区块链B_A、B_B、B_C，用于存储各自的工业设备传感器采集到的数据。因为数据保密的等级不同，区块链上可存储的性能有限，所以传感器返回的信息会根据其保密等级及大小存储在不同区块上，如A企业有摄像头1、摄像头2、摄像头3、工控设备1、工控设备2、工控设备3、温度传感器1、温度传感器2、温度传感器3等。温度传感器数据量相对小一点，B_A上的一个区块可存储一个温度传感器一天的数据，而摄像头作为大流量数据的传感器，可能一个区块只能存储两小时回传的数据。工控设备传入的数据因保密级别较高，可能需要存储区块链B_A的非共享区块上。其他两个企业B、C类似，将采集到的数据存储在区块链B_B、B_C上。

[0083] 2)数据共享阶段。该阶段主要是企业确定哪些数据可以参与共享，将可以共享的区块对应的标志设置为1。等待用户确定数据训练模型。当有用户上传数据训练模型M_{fed}到共享区块链SB后，SB生成新的区块存储训练模型，然后通过同态加密算法加密模型M_{fed}，并将加密后的模型M_{fed}下发到企业A、B、C的区块链B_A、B_B、B_C上，分别生成新的区块。然后区块链B_A、B_B、B_C上根据模型M_{fed}训练数据，并将结果进行加密，加密方法参考第3节介绍相关知识。并将训练后的结果参数返回给共享区块链SB，SB接收到数据后，解密并整合企业A、B、C返回

的数据，再次根据模型M_{fed}进行运算，并生成新的区块存储最终训练结果。

[0084] 3)查询使用阶段。当共享区块链SB计算完成最终训练结果后，会给用户返回一个完成的信息。此时用户可以根据自己的情况下载查询训练后的结果并使用结果，或者用户可以选择上传新的模型重新进行计算。

[0085] 最后说明的是，以上实施例仅用以说明本发明的技术方案而非限制，尽管参照较佳实施例对本发明进行了详细说明，本领域的普通技术人员应当理解，可以对本发明的技术方案进行修改或者等同替换，而不脱离本技术方案的宗旨和范围，其均应涵盖在本发明的权利要求范围当中。

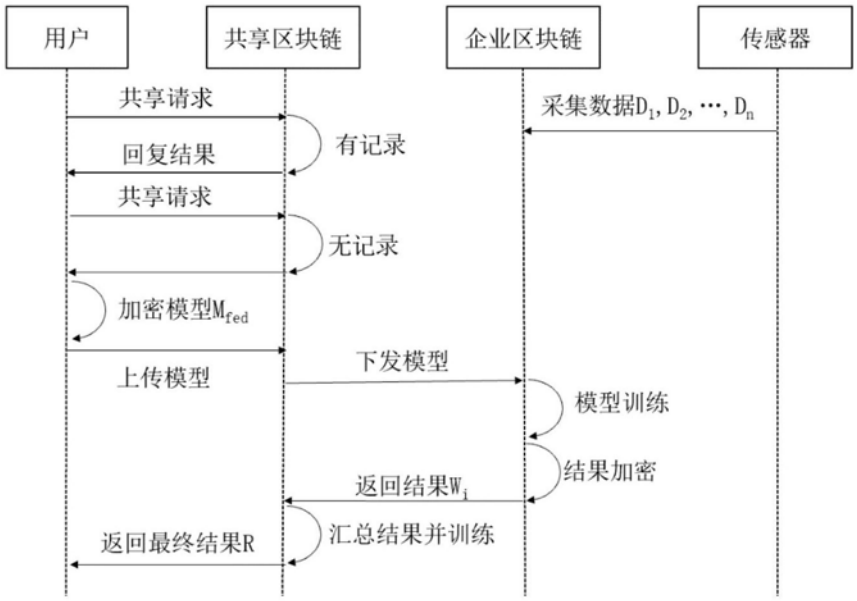

用户
共享区块链
企业区块链
传感器
共享请求
采集数据$D_1, D_2, \cdots, D_n$
回复结果
有记录
共享请求
无记录
加密模型M_{fed}
上传模型
下发模型
模型训练
结果加密
返回结果W_i
返回最终结果R
汇总结果并训练

图1

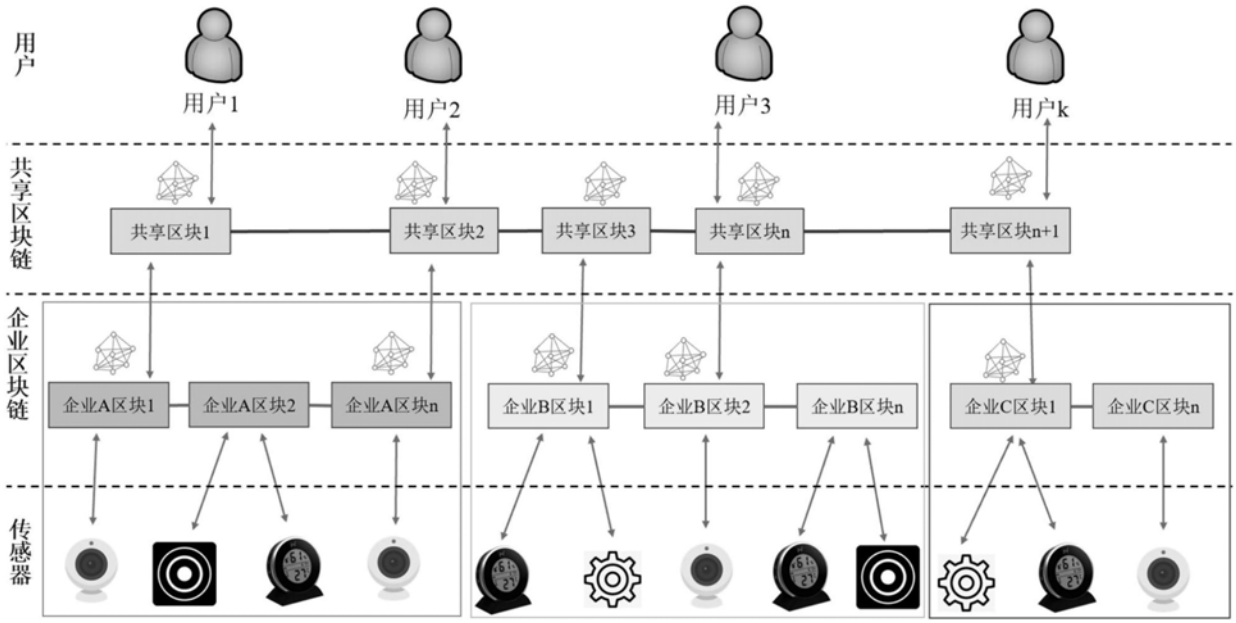

用户
用户1
用户2
用户3
用户k
共享区块链
共享区块1
共享区块2
共享区块3
共享区块n
共享区块n+1
企业区块链
企业A区块1
企业A区块2
企业A区块n
企业B区块1
企业B区块2
企业B区块n
企业C区块1
企业C区块n
传感器

图2