

(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
2020 年 9 月 10 日 (10.09.2020)



(10) 国际公布号
WO 2020/177392 A1

(51) 国际专利分类号:
G06N 20/00 (2019.01) G06F 21/60 (2013.01)

(21) 国际申请号: PCT/CN2019/119227

(22) 国际申请日: 2019 年 11 月 18 日 (18.11.2019)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201910158538.8 2019 年 3 月 1 日 (01.03.2019) 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: 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)。 杨强 (YANG, Qiang); 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粤海街道高新技术产业园北区松坪山路 3 号奥特讯电力大厦 201, Guangdong 518057 (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,

(54) Title: FEDERATED LEARNING-BASED MODEL PARAMETER TRAINING METHOD, APPARATUS AND DEVICE, AND MEDIUM

(54) 发明名称: 基于联邦学习的模型参数训练方法、装置、设备及介质

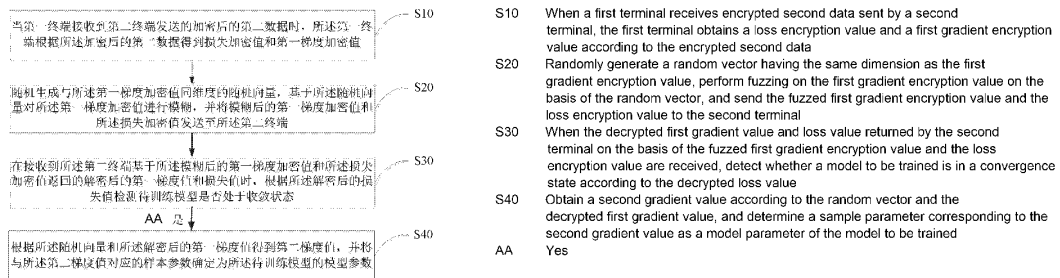


图 2

(57) Abstract: Disclosed in the present application are a federated learning-based model parameter training method, apparatus and device, and a medium. The method comprises: when a first terminal receives encrypted second data sent by a second terminal, obtaining a corresponding loss encryption value and a first gradient encryption value; randomly generating a random vector having the same dimension as the first gradient encryption value, performing fuzzing on the first gradient encryption value on the basis of the random vector, and sending the fuzzed first gradient encryption value and the loss encryption value to the second terminal; when the decrypted first gradient value and loss value returned by the second terminal are received, detecting whether a model to be trained is in a convergence state according to the decrypted loss value; and if yes, obtaining a second gradient value according to the random vector and the decrypted first gradient value, and determining a sample parameter corresponding to the second gradient value as a model parameter.

(57) 摘要: 本申请公开了一种基于联邦学习的模型参数训练方法、装置、设备及介质。该方法包括: 当第一终端接收到第二终端发送的加密后的第二数据时, 获取对应的损失加密值和第一梯度加密值; 随机生成与第一梯度加密值同维度的随机向量, 基于随机向量对第一梯度加密值进行模糊, 并将模糊后的第一梯度加密值和损失加密值发送至第二终端; 在接收到第二终端返回的解密后的第一梯度值和损失值时, 根据解密后的损失值检测待训练模型是否处于收敛状态; 若是, 则根据随机向量和解密后的第一梯度值得到第二梯度值, 并将与第二梯度值对应的样本参数确定为模型参数。

[见续页]

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, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, 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, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, 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))。