

(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



(10) 国际公布号
WO 2023/154005 A3

(43) 国际公布日
2023 年 8 月 17 日 (17.08.2023)

- (51) 国际专利分类号:
G06N 20/20 (2019.01) *G06N 3/08* (2023.01)
G06F 21/60 (2013.01)
- (21) 国际申请号: PCT/SG2023/050057
- (22) 国际申请日: 2023 年 2 月 2 日 (02.02.2023)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
202210119229.1 2022 年 2 月 8 日 (08.02.2022) CN
- (71) 申请人: 脸萌有限公司 (LEMON INC.) [GB/SG]; 开曼群岛大开曼西湾路 802 号木槿道大楼邮政信箱 31119, Grand Cayman KY1 - 1205 (KY)。
- (72) 发明人: 孙建凯 (SUN, Jiankai); 美国加利福尼亚州洛杉矶西杰弗逊大道 12655 号六层第 137 室,

California 90066 (US)。杨鑫 (YANG, Xin); 美国加利福尼亚州洛杉矶西杰弗逊大道 12655 号六层第 137 室, California 90066 (US)。姚元舜 (YAO, Yuanshun); 美国加利福尼亚州洛杉矶西杰弗逊大道 12655 号六层第 137 室, California 90066 (US)。解浚源 (XIE, Junyuan); 中国北京市海淀区知春路 63 号中国卫星通信大厦今日头条小邮局, Beijing 100086 (CN)。王崇 (WANG, Chong); 美国加利福尼亚州洛杉矶西杰弗逊大道 12655 号六层第 137 室, California 90066 (US)。

- (74) 代理人: 傅子健 (POH, Chee Kian, Daniel); 新加坡新加坡麦仕奇新加坡, 丹戎巴葛邮局, POBox636, Singapore 910816 (SG)。
- (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, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU,

(54) Title: METHOD AND APPARATUS FOR PROTECTING DATA, AND DEVICE AND MEDIUM

(54) 发明名称: 用于保护数据的方法、设备、装置和介质

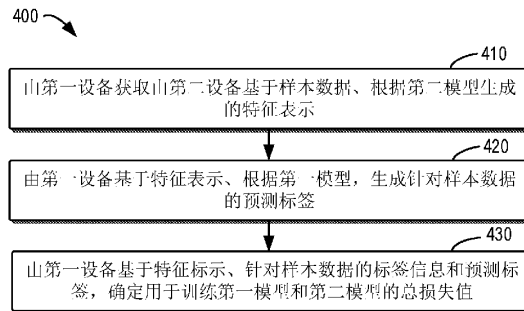


图 4

- 410 Acquire, by a first device, a feature representation generated by a second device on the basis of sample data and according to a second model
- 420 Generate, by the first device, a prediction label for the sample data on the basis of the feature representation and according to a first model
- 430 Determine, by the first device and on the basis of the feature representation, label information for the sample data and the prediction label, a total loss value used for training the first model and the second model

(57) Abstract: According to the embodiments of the present disclosure, a method and apparatus for protecting data, and a device and a medium are provided. The method comprises acquiring, by a first device, a feature representation generated by a second device on the basis of sample data and according to a second model, wherein the first device has label information for the sample data; and the first device and the second device are used for jointly training a first model at the first device and the second model at the second device. The method further comprises generating, by the first device, a prediction label for the sample data on the basis of the feature representation and according to the first model. The method further comprises determining, by the first device and on the basis of

[见续页]

WO 2023/154005 A3

CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, 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, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, 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, CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SC, 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, ME, 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))。
- 在修改权利要求的期限届满之前进行, 在收到该修改后将重新公布(细则48.2(h))。

(88) 国际检索报告公布日期:

2023 年 11 月 2 日 (02.11.2023)

the feature representation, the label information and the prediction label, a total loss value used for training the first model and the second model. In this way, a second device, which does not have label information of data, can be prevented from predicting the label information of the data, thereby protecting data, especially sensitive data, from being leaked.

(57) 摘要: 根据本公开的实施例, 提供了用于保护数据的方法、设备、装置和介质。该方法包括由第一设备获取由第二设备基于样本数据、根据第二模型生成的特征表示。第一设备具有针对样本数据的标签信息。第一设备和第二设备用于联合训练第一设备处的第一模型和第二设备处的第二模型。该方法还包括由第一设备基于特征表示, 根据第一模型, 生成针对样本数据的预测标签。该方法还包括由第一设备基于特征表示、标签信息和预测标签, 来确定用于训练第一模型和第二模型的总损失值。以此方式, 能够避免不具有数据的标签信息的第二设备对数据的标签信息进行预测, 从而保存数据尤其是敏感数据不被泄露。