(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 111475855 B
(45)授权公告日 2020.12.25

(21)申请号 202010590733.0
(22)申请日 2020.06.24
(65)同一申请的已公布的文献号
申请公布号 CN 111475855 A
(43)申请公布日 2020.07.31
(73)专利权人 支付宝(杭州)信息技术有限公司
地址 310000 浙江省杭州市西湖区西溪路556号8层B段801-11
(72)发明人 李龙飞 周俊
(74)专利代理机构 北京亿腾知识产权代理事务所(普通合伙) 11309
代理人 陈婧玥 周良玉
(51)Int.Cl.
G06F 21/62(2013.01)

审查员 朱江岩

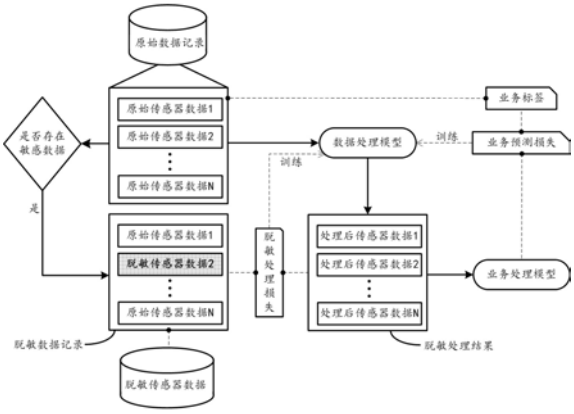
权利要求书4页 说明书12页 附图6页

(54)发明名称

实现隐私保护的数据处理方法及装置

(57)摘要

本说明书实施例提供一种实现隐私保护的数据处理方法，包括：先获取多个终端传感器采集到的多条原始传感器数据，构成原始数据记录，以及获取对应的针对用户的业务标签；然后，判断该原始数据记录中是否包含反映用户做出特定隐私行为的敏感传感器数据；在判断出包含的情况下，利用中性数据进行对应局部替换得到脱敏数据记录，并将上述原始数据记录输入数据脱敏模型，得到脱敏处理结果；进一步地，一方面，基于该脱敏处理结果和该脱敏数据记录，确定脱敏处理损失，另一方面，将该脱敏处理结果输入预先训练的业务预测模型中，得到业务预测结果，并结合上述业务标签确定业务预测损失；进而基于脱敏处理损失和业务预测损失，训练数据脱敏模型。



CN 111475855 B

1.一种实现隐私保护的数据处理方法,包括:

获取原始数据记录和对应的业务标签;所述原始数据记录中包括多条原始传感器数据,其由用户终端中的多个传感器进行采集而得到;所述业务标签对应针对用户的业务预测任务,所述业务预测任务至少包括以下中的一项任务:健康指标预测、运动状态识别、设备轨迹识别;

判断所述原始数据记录中是否包含敏感传感器数据,该敏感传感器数据反映用户做出若干特定隐私行为中的至少一种;

在判断出包含若干条敏感传感器数据的情况下,利用预先确定的若干条脱敏传感器数据,替换所述原始数据记录中的所述若干条敏感传感器数据,得到脱敏数据记录,其中若干条敏感传感器数据和若干条脱敏传感器数据对应相同的若干个传感器;

将所述原始数据记录输入数据脱敏模型,得到脱敏处理结果;

基于所述脱敏处理结果和所述脱敏数据记录,确定脱敏处理损失;

将所述脱敏处理结果输入业务预测模型中,得到业务预测结果,所述业务预测模型用于执行所述业务预测任务,所述业务预测模型基于多条原始数据记录和对应的多个业务标签进行预先训练而得到;

基于所述业务预测结果和所述业务标签,确定业务预测损失;

基于所述脱敏处理损失和业务预测损失,训练所述数据脱敏模型;训练后的数据脱敏模型用于对目标原始数据记录进行脱敏处理。

2.根据权利要求1所述的方法,其中各条原始传感器数据包括观测值序列,该观测值序列由传感器在多个预定时刻采集到的多个观测值组成。

3.根据权利要求1所述的方法,其中,所述多个传感器中包括以下中的至少一个:重力传感器,位置传感器,加速度传感器,角速度传感器,心率传感器。

4.根据权利要求1所述的方法,其中,所述若干特定隐私行为包括用户设定的禁止采集的行为和/或用户未授权采集的行为,所述业务预测任务对应用户授权的业务。

5.根据权利要求1所述的方法,其中,所述若干特定隐私行为中包括第一隐私行为;其中,判断所述原始数据记录中是否包含敏感传感器数据,包括:

基于预先设定的传感器与特定隐私行为之间的映射关系,从所述多条原始传感器数据中确定与所述第一隐私行为对应的若干条第一原始数据;

基于所述若干条第一原始数据,判断用户是否做出所述第一隐私行为;

在判断出用户做出所述第一隐私行为的情况下,将所述若干条第一原始数据归入所述若干条敏感传感器数据中。

6.根据权利要求5所述的方法,其中,基于所述若干条第一原始数据,判断用户是否做出所述第一隐私行为,包括:

将所述若干条第一原始数据输入预先训练的第一行为预测模型中,得到预测结果,指示用户是否做出所述第一隐私行为。

7.根据权利要求5所述的方法,其中,基于所述若干条第一原始数据,判断用户是否做出所述第一隐私行为,包括:

判断其中各条第一原始数据是否在各自对应的预设区间内;

在判断出均在各自对应的预设区间内的情况下,判定用户做出所述第一隐私行为。

8.根据权利要求1所述的方法，其中，所述若干条脱敏传感器数据中包括对应于第一传感器的第一脱敏传感器数据，其基于以下步骤预先确定：

获取多条第一原始传感器数据，其由多个用户终端中的多个第一传感器采集得到；

对所述多条第一原始传感器数据进行平均处理，得到所述第一脱敏传感器数据。

9.一种实现隐私保护的数据处理方法，包括：

获取原始数据记录和对应的业务标签；所述原始数据记录中包括多条原始传感器数据，其由用户终端中的多个传感器进行采集而得到；所述业务标签对应针对用户的业务预测任务，所述业务预测任务至少包括以下中的一项任务：健康指标预测、运动状态识别、设备轨迹识别；

获取预先确定的与若干传感器对应的若干条脱敏传感器数据，其中若干传感器采集的原始数据可用于推断用户的特定隐私信息；

利用所述若干条脱敏传感器数据，对所述原始数据记录中与所述若干传感器对应的若干条原始传感器数据进行替换，得到脱敏数据记录；

将所述原始数据记录输入数据脱敏模型，得到脱敏处理结果；

基于所述脱敏处理结果和所述脱敏数据记录，确定脱敏处理损失；

将所述脱敏处理结果输入业务预测模型中，得到业务预测结果，所述业务预测模型用于执行所述业务预测任务，所述业务预测模型基于多条原始数据记录和对应的多个业务标签进行预先训练而得到；

基于所述业务预测结果和所述业务标签，确定业务预测损失；

基于所述脱敏处理损失和业务预测损失，训练所述数据脱敏模型；训练后的数据脱敏模型用于对目标原始数据记录进行脱敏处理。

10.根据权利要求9所述的方法，其中，所述特定隐私信息包括性别和/或年龄。

11.一种实现隐私保护的数据处理装置，包括：

获取单元，配置为获取原始数据记录和对应的业务标签；所述原始数据记录中包括多条原始传感器数据，其由用户终端中的多个传感器进行采集而得到；所述业务标签对应针对用户的业务预测任务，所述业务预测任务至少包括以下中的一项任务：健康指标预测、运动状态识别、设备轨迹识别；

判断单元，配置为判断所述原始数据记录中是否包含敏感传感器数据，该敏感传感器数据反映用户做出若干特定隐私行为中的至少一种；

替换单元，配置为在判断出包含若干条敏感传感器数据的情况下，利用预先确定的若干条脱敏传感器数据，替换所述原始数据记录中的所述若干条敏感传感器数据，得到脱敏数据记录，其中若干条敏感传感器数据和若干条脱敏传感器数据对应相同的若干个传感器；

脱敏单元，配置为将所述原始数据记录输入数据脱敏模型，得到脱敏处理结果；

脱敏损失确定单元，配置为基于所述脱敏处理结果和所述脱敏数据记录，确定脱敏处理损失；

业务预测单元，配置为将所述脱敏处理结果输入业务预测模型中，得到业务预测结果，所述业务预测模型用于执行所述业务预测任务，所述业务预测模型基于多条原始数据记录和对应的多个业务标签进行预先训练而得到；

业务损失确定单元，配置为基于所述业务预测结果和所述业务标签，确定业务预测损失；

模型训练单元，配置为基于所述脱敏处理损失和业务预测损失，训练所述数据脱敏模型；训练后的数据脱敏模型用于对目标原始数据记录进行脱敏处理。

12.根据权利要求11所述的装置，其中各条原始传感器数据包括观测值序列，该观测值序列由传感器在多个预定时刻采集到的多个观测值组成。

13.根据权利要求11所述的装置，其中，所述多个传感器中包括以下中的至少一个：重力传感器，位置传感器，加速度传感器，角速度传感器，心率传感器。

14.根据权利要求11所述的装置，其中，所述若干特定隐私行为包括用户设定的禁止采集的行为和/或用户未授权采集的行为，所述业务预测任务对应用户授权的业务。

15.根据权利要求11所述的装置，其中，所述若干特定隐私行为中包括第一隐私行为；所述判断单元具体包括：

确定子单元，配置为基于预先设定的传感器与特定隐私行为之间的映射关系，从所述多条原始传感器数据中确定与所述第一隐私行为对应的若干条第一原始数据；

判断子单元，配置为基于所述若干条第一原始数据，判断用户是否做出所述第一隐私行为；

归入子单元，配置为在判断出用户做出所述第一隐私行为的情况下，将所述若干条第一原始数据归入所述若干条敏感传感器数据中。

16.根据权利要求15所述的装置，其中，所述判断子单元具体配置为：

将所述若干条第一原始数据输入预先训练的第一行为预测模型中，得到预测结果，指示用户是否做出所述第一隐私行为。

17.根据权利要求15所述的装置，其中，所述判断子单元具体配置为：

判断其中各条第一原始数据是否在各自对应的预设区间内；

在判断出均在各自对应的预设区间内的情况下，判定用户做出所述第一隐私行为。

18.根据权利要求11所述的装置，其中，所述若干条脱敏传感器数据中包括对应于第一传感器的第一脱敏传感器数据，其基于数据确定单元而得到，所述数据确定单元配置为：

获取多条第一原始传感器数据，其由多个用户终端中的多个第一传感器采集得到；

对所述多条第一原始传感器数据进行平均处理，得到所述第一脱敏传感器数据。

19.一种实现隐私保护的数据处理装置，包括：

第一获取单元，配置为获取原始数据记录和对应的业务标签；所述原始数据记录中包括多条原始传感器数据，其由用户终端中的多个传感器进行采集而得到；所述业务标签对应针对用户的业务预测任务，所述业务预测任务至少包括以下中的一项任务：健康指标预测、运动状态识别、设备轨迹识别；

第二获取单元，配置为获取预先确定的与若干传感器对应的若干条脱敏传感器数据，其中若干传感器采集的原始数据可用于推断用户的特定隐私信息；

替换单元，配置为利用所述若干条脱敏传感器数据，对所述原始数据记录中与所述若干传感器对应的若干条原始传感器数据进行替换，得到脱敏数据记录；

脱敏单元，配置为将所述原始数据记录输入数据脱敏模型，得到脱敏处理结果；

脱敏损失确定单元，配置为基于所述脱敏处理结果和所述脱敏数据记录，确定脱敏处

理损失；

业务预测单元，配置为将所述脱敏处理结果输入业务预测模型中，得到业务预测结果，所述业务预测模型用于执行所述业务预测任务，所述业务预测模型基于多条原始数据记录和对应的多个业务标签进行预先训练而得到；

业务损失确定单元，配置为基于所述业务预测结果和所述业务标签，确定业务预测损失；

模型训练单元，配置为基于所述脱敏处理损失和业务预测损失，训练所述数据脱敏模型；训练后的数据脱敏模型用于对目标原始数据记录进行脱敏处理。

20.根据权利要求19所述的装置，其中，所述特定隐私信息包括性别和/或年龄。

21.一种计算机可读存储介质，其上存储有计算机程序，其中，当所述计算机程序在计算机中执行时，令计算机执行权利要求1-10中任一项的所述的方法。

22.一种计算设备，包括存储器和处理器，其中，所述存储器中存储有可执行代码，所述处理器执行所述可执行代码时，实现权利要求1-10中任一项所述的方法。

实现隐私保护的数据处理方法及装置

技术领域

[0001] 本说明书一个或多个实施例涉及数据安全技术领域，尤其涉及一种实现隐私保护的数据处理方法及装置。

背景技术

[0002] 目前，个人智能设备中嵌入有许多传感器，包括加速度计、陀螺仪和磁力计等，安装在智能设备上的应用程序APP可以访问这些传感器采集到的原始数据，并对原始传感器数据进行处理，以实现与用户的交互，或计算展示给用户的指标数据，以帮助用户了解自己的活动情况或身体状态等。

[0003] 然而，丰富的原始传感器数据同样带来了泄露用户隐私的风险，比如，用户希望保护自己某些方的隐私，如性别、年龄、某些个人行为习惯(如抽烟)等，但是一些APP可能会对原始传感器数据进行非法或恶意的使用、推测，从而造成用户隐私泄露。

[0004] 因此，需要一种方案，使得传感器数据在可以正常用于后续业务处理的同时，防止用户隐私信息的泄露，从而有效保障用户隐私安全。

发明内容

[0005] 本说明书一个或多个实施例描述了一种实现隐私保护的数据处理方法及装置，通过对原始传感器数据进行脱敏处理，从而有效保障用户隐私安全，同时，保证脱敏处理后的传感器数据，对于后续的业务处理仍具有足够高的可用性。

[0006] 根据第一方面，提供一种实现隐私保护的数据处理方法，包括：获取原始数据记录和对应的业务标签；所述原始数据记录中包括多条原始传感器数据，其由用户终端中的多个传感器进行采集而得到；所述业务标签对应针对用户的业务预测任务。判断所述原始数据记录中是否包含敏感传感器数据，该敏感传感器数据反映用户做出若干特定隐私行为中的至少一种。在判断出包含若干条敏感传感器数据的情况下，利用预先确定的若干条脱敏传感器数据，替换所述原始数据记录中的所述若干条敏感传感器数据，得到脱敏数据记录，其中若干条敏感传感器数据和若干条脱敏传感器数据对应相同的若干个传感器。将所述原始数据记录输入数据脱敏模型，得到脱敏处理结果。基于所述脱敏处理结果和所述脱敏数据记录，确定脱敏处理损失。将所述脱敏处理结果输入预先训练的业务预测模型中，得到业务预测结果，所述业务预测模型用于执行所述业务预测任务。基于所述业务预测结果和所述业务标签，确定业务预测损失。基于所述脱敏处理损失和业务预测损失，训练所述数据脱敏模型，训练后的数据脱敏模型用于对目标原始数据记录进行脱敏处理。

[0007] 在一个实施例中，其中各条原始传感器数据包括观测值序列，该观测值序列由传感器在多个预定时刻采集到的多个观测值组成。

[0008] 在一个实施例中，所述多个传感器中包括以下中的至少一个：重力传感器，位置传感器，加速度传感器，角速度传感器，心率传感器。

[0009] 在一个实施例中，所述若干特定隐私行为包括用户设定的禁止采集的行为和/或

用户未授权采集的行为，所述业务预测任务对应用户授权的业务。

[0010] 在一个实施例中，所述若干特定隐私行为中包括第一隐私行为；其中，判断所述原始数据记录中是否包含敏感传感器数据，包括：基于预先设定的传感器与特定隐私行为之间的映射关系，从所述多条原始传感器数据中确定与所述第一隐私行为对应的若干条第一原始数据；基于所述若干条第一原始数据，判断用户是否做出所述第一隐私行为；在判断出用户做出所述第一隐私行为的情况下，将所述若干条第一原始数据归入所述若干条敏感传感器数据中。

[0011] 在一个具体的实施例中，基于所述若干条第一原始数据，判断用户是否做出所述第一隐私行为，包括：将所述若干条第一原始数据输入预先训练的第一行为预测模型中，得到预测结果，指示用户是否做出所述第一隐私行为。

[0012] 在一个具体的实施例中，基于所述若干条第一原始数据，判断用户是否做出所述第一隐私行为，包括：判断其中各条第一原始数据是否在各自对应的预设区间内；在判断出均在各自对应的预设区间内的情况下，判定用户做出所述第一隐私行为。

[0013] 在一个实施例中，所述若干条脱敏传感器数据中包括对应于第一传感器的第一脱敏传感器数据，其基于以下步骤预先确定：获取多条第一原始传感器数据，其由多个用户终端中的多个第一传感器采集得到；对所述多条第一原始传感器数据进行平均处理，得到所述第一脱敏传感器数据。

[0014] 在一个实施例中，所述业务预测模型基于多条原始数据记录和对应的多个业务标签进行预先训练而得到。

[0015] 根据第二方面，提供一种实现隐私保护的数据处理方法，包括：获取原始数据记录和对应的业务标签；所述原始数据记录中包括多条原始传感器数据，其由用户终端中的多个传感器进行采集而得到；所述业务标签对应针对用户的业务预测任务；获取预先确定的与若干传感器对应的若干条脱敏传感器数据，其中若干传感器采集的原始数据可用于推断用户的特定隐私信息；利用所述若干条脱敏传感器数据，对所述原始数据记录中与所述若干传感器对应的若干条原始传感器数据进行替换，得到脱敏数据记录；将所述原始数据记录输入数据脱敏模型，得到脱敏处理结果；基于所述脱敏处理结果和所述脱敏数据记录，确定脱敏处理损失；将所述脱敏处理结果输入预先训练的业务预测模型中，得到业务预测结果，所述业务预测模型用于执行所述业务预测任务；基于所述业务预测结果和所述业务标签，确定业务预测损失；基于所述第一脱敏处理损失和业务预测损失，训练所述数据脱敏模型；训练后的数据脱敏模型用于对目标原始数据记录进行脱敏处理。

[0016] 在一个实施例中，所述特定隐私信息包括性别和/或年龄。

[0017] 根据第三方面，提供一种实现隐私保护的数据处理装置，包括：获取单元，配置为获取原始数据记录和对应的业务标签；所述原始数据记录中包括多条原始传感器数据，其由用户终端中的多个传感器进行采集而得到；所述业务标签对应针对用户的业务预测任务；判断单元，配置为判断所述原始数据记录中是否包含敏感传感器数据，该敏感传感器数据反映用户做出若干特定隐私行为中的至少一种；替换单元，配置为在判断出包含若干条敏感传感器数据的情况下，利用预先确定的若干条脱敏传感器数据，替换所述原始数据记录中的所述若干条敏感传感器数据，得到脱敏数据记录，其中若干条敏感传感器数据和若干条脱敏传感器数据对应相同的若干个传感器；脱敏单元，配置为将所述原始数据记录输

入数据脱敏模型，得到脱敏处理结果；脱敏损失确定单元，配置为基于所述脱敏处理结果和所述脱敏数据记录，确定脱敏处理损失；业务预测单元，配置为将所述脱敏处理结果输入预先训练的业务预测模型中，得到业务预测结果，所述业务预测模型用于执行所述业务预测任务；业务损失确定单元，配置为基于所述业务预测结果和所述业务标签，确定业务预测损失；模型训练单元，配置为基于所述脱敏处理损失和业务预测损失，训练所述数据脱敏模型；训练后的数据脱敏模型用于对目标原始数据记录进行脱敏处理。

[0018] 根据第四方面，提供一种实现隐私保护的数据处理装置，包括：第一获取单元，配置为获取原始数据记录和对应的业务标签；所述原始数据记录中包括多条原始传感器数据，其由用户终端中的多个传感器进行采集而得到；所述业务标签对应针对用户的业务预测任务；第二获取单元，配置为获取预先确定的与若干传感器对应的若干条脱敏传感器数据，其中若干传感器采集的原始数据可用于推断用户的特定隐私信息；替换单元，配置为利用所述若干条脱敏传感器数据，对所述原始数据记录中与所述若干传感器对应的若干条原始传感器数据进行替换，得到脱敏数据记录；脱敏单元，配置为将所述原始数据记录输入数据脱敏模型，得到脱敏处理结果；脱敏损失确定单元，配置为基于所述脱敏处理结果和所述脱敏数据记录，确定脱敏处理损失；业务预测单元，配置为将所述脱敏处理结果输入预先训练的业务预测模型中，得到业务预测结果，所述业务预测模型用于执行所述业务预测任务；业务损失确定单元，配置为基于所述业务预测结果和所述业务标签，确定业务预测损失；模型训练单元，配置为基于所述第一脱敏处理损失和业务预测损失，训练所述数据脱敏模型；训练后的数据脱敏模型用于对目标原始数据记录进行脱敏处理。

[0019] 根据第五方面，提供了一种计算机可读存储介质，其上存储有计算机程序，当所述计算机程序在计算机中执行时，令计算机执行上述第一方面或第二方面的方法。

[0020] 根据第六方面，提供了一种计算设备，包括存储器和处理器，所述存储器中存储有可执行代码，所述处理器执行所述可执行代码时，实现上述第一方面或第二方面的方法。

[0021] 综上，在本说明书实施例提供的上述方法及装置中，可以实现对原始传感器数据的脱敏处理，从而防止用户隐私行为等用户隐私信息的泄露，保障用户隐私安全，同时，保证脱敏处理后的传感器数据，可以被正常用于相关业务的处理，在业务处理中具有足够高的可用性。

附图说明

[0022] 为了更清楚地说明本发明实施例的技术方案，下面将对实施例描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其它的附图。

[0023] 图1示出根据一个实施例的数据脱敏模型的训练实施架构图；

[0024] 图2示出根据一个实施例的实现隐私保护的数据处理方法的流程示意图；

[0025] 图3示出根据另一个实施例的数据脱敏模型的训练实施架构图；

[0026] 图4示出根据另一个实施例的实现隐私保护的数据处理方法的流程示意图；

[0027] 图5示出根据一个实施例的实现隐私保护的数据处理方装置的结构图；

[0028] 图6示出根据另一个实施例的实现隐私保护的数据处理方装置的结构图。

具体实施方式

[0029] 下面结合附图，对本说明书提供的方案进行描述。

[0030] 本说明书实施例披露一种实现隐私保护的数据处理方法，通过对原始传感器数据进行脱敏处理，可以实现对用户特定隐私信息的保护。随着机器学习的兴起，发明人想到，可以将机器学习技术应用到数据隐私安全的技术领域，通过训练出用于对原始传感器数据进行脱敏处理的机器学习模型(以下简称数据脱敏模型)，实现对数据隐私的保护。

[0031] 图1示出根据一个实施例的数据脱敏模型的训练实施架构图，如图1所示，对于用户终端中包括的多个传感器(图1中示出N个，N为大于1的整数)，各个传感器各自进行数据采集，对应得到N条原始传感器数据，基于此，可以获取该N条原始传感器数据，构成原始数据记录；然后，判断原始数据记录中是否包含敏感传感器数据，该敏感传感器数据反映用户做出特定隐私行为(例如，抽烟)；在判断出包含若干条敏感传感器数据的情况下，利用预先确定的若干条脱敏传感器数据，替换上述原始数据记录中的若干条敏感传感器数据，得到脱敏数据记录，其中若干条脱敏传感器数据与若干条敏感传感器数据对应相同的若干个传感器；然后，将原始数据记录输入数据脱敏模型中，得到脱敏处理结果；接着，一方面，基于脱敏处理结果和脱敏数据记录确定脱敏处理损失，另一方面，将脱敏处理结果输入预先训练的业务预测模型中，得到业务预测结果(例如，步行模式)，并基于业务预测结果和与原始数据记录对应的业务标签，确定业务预测损失；进一步地，基于脱敏处理损失和业务预测损失，训练上述数据脱敏模型。

[0032] 通过多次迭代训练，可以得到训练好的数据脱敏模型，用于对目标原始数据记录进行脱敏处理，并在终端APP或其他访问方调用传感器数据时，提供脱敏处理后的传感器数据，从而实现有效地防止用户隐私行为的泄露，实现用户隐私保护。

[0033] 下面结合实施例，描述上述方法的具体实施步骤。

[0034] 图2示出根据一个实施例的实现隐私保护的数据处理方法的流程示意图，所述方法的执行主体可以为任何具有计算、处理能力的装置或平台或设备集群。如图2所示，所述方法包括以下步骤：

[0035] 步骤S210，获取原始数据记录和对应的业务标签；该原始数据记录中包括多条原始传感器数据，其由用户终端中的多个传感器进行采集而得到；该业务标签对应针对用户的业务预测任务；步骤S220，判断该原始数据记录中是否包含敏感传感器数据，该敏感传感器数据反映用户做出若干特定隐私行为中的至少一种；步骤S230，在判断出包含若干条敏感传感器数据的情况下，利用预先确定的若干条脱敏传感器数据，替换该原始数据记录中的该若干条敏感传感器数据，得到脱敏数据记录，其中若干条敏感传感器数据和若干条脱敏传感器数据对应相同的若干个传感器；步骤S240，将该原始数据记录输入数据脱敏模型，得到脱敏处理结果；步骤S250，基于该脱敏处理结果和该脱敏数据记录，确定脱敏处理损失；步骤S260，将该脱敏处理结果输入预先训练的业务预测模型中，得到业务预测结果，该业务预测模型用于执行该业务预测任务；步骤S270，基于该业务预测结果和该业务标签，确定业务预测损失；步骤S280，基于该脱敏处理损失和业务预测损失，训练该数据脱敏模型；训练后的数据脱敏模型用于对目标原始数据记录进行脱敏处理。

[0036] 针对以上步骤，首先需要说明，文中的“若干”均指代一个或多个。以上步骤具体如下：

[0037] 首先，在步骤S210，获取原始数据记录和对应的业务标签。

[0038] 用户终端中配置多个传感器，其中各个传感器各自进行数据的采集，得到对应的一条原始传感器数据，于是用户终端中存储多个传感器采集到的多条传感器数据，组成上述原始数据记录，由此可以对其进行获取。

[0039] 在一个实施例中，其中用户终端可以包括智能手机、平板电脑、可穿戴设备(如智能手表、智能手环、智能眼镜)等。

[0040] 在一个实施例中，其中多个传感器可以包括运动传感器、生物传感器和环境传感器。在一个具体的实施例中，其中运动传感器可以包括重力传感器、位置传感器、加速度传感器、角速度传感器(如陀螺仪)、地磁传感器。在一个具体的实施例中，其中生物传感器可以包括血糖传感器、血压传感器、心率传感器、肌电传感器、体温传感器、脑电波传感器。在一个具体的实施例中，其中环境传感器可以包括土壤温度传感器、空气温湿度传感器、蒸发传感器、雨量传感器、光照传感器、风速风向传感器等。

[0041] 在一个实施例中，其中各条原始传感器数据包括观测值序列，该观测值序列由对应传感器在多个预定时刻采集到的多个观测值组成。需要理解，对于上述多条原始传感器数据，其中各条原始传感器数据对应的多个采集时刻通常是相同的。在一个具体的实施例中，原始数据记录可以包括一个M行W列的矩阵，其中M表示多个传感器的数量，矩阵中的一行数值对应上述一条原始传感器数据，其中W表示观测值数量，也就是上述多个预定时刻的数量，其中每一列对应一个预定的采集时刻。在另一个实施例中，其中各条原始传感器数据包括初步计算值或初步计算值序列。比如，对预定时段内按照预定时间间隔采集到的多个数据进行平均或加和处理，得到对应的初步计算值，或者，对预定时段采集到的多个数据(例如，1min内采集到60个数值)进行分段平均(例如，每10个数值作为一个分段)，得到对应的初步计算值序列(例如，由6个初步计算值组成)。如此，可以得到各条原始传感器数据，进而组成上述原始数据记录。

[0042] 另一方面，上述业务标签对应针对用户的业务预测任务。在一个实施例中，该业务预测任务对应用户授权的业务。通常，在施行某项业务时，通常会通过终端界面的交互选项寻求用户的授权许可，由此可以获悉用户的授权操作或禁止操作，进而根据用户授权的业务实施业务预测任务，向用户提供预测得到的业务数据。在另一个实施例中，该业务预测任务所对应的业务，可以是工作人员根据大数据分析出来的，用户通常会授权的业务。比如说，用户通常比较关注自身健康指标，如心率、血氧、血压、运动状态(或称运动模式)等，由此可以针对其中不能根据传感器数据直接得到，而是需要根据传感器数据进行分析的指标设计业务预测任务，如运动状态监测。又比如说，用户可以利用智能终端的轨迹识别触发交互指令，其中轨迹可以是手握终端或手腕上戴着终端设备进行运动时产生的运动轨迹，此时，可以将轨迹识别归入上述业务预测任务。需要说明，上述业务预测任务可以是一个或多个，相应地，业务标签也可是一个或多个。根据一个具体的实施例，上述业务预测任务包括运动模式识别，则上述业务标签可以包括步行或跑步。根据另一个具体的实施例，上述业务预测任务包括手部轨迹识别，则上述业务标签可以包括用户终端中预置的几种运动轨迹中的一种。

[0043] 由上，可以获取由传感器采集的原始数据组成的原始数据记录和对应的业务标签。

[0044] 接着，在步骤S220，判断该原始数据记录中是否包含敏感传感器数据，该敏感传感器数据反映用户做出若干特定隐私行为中的至少一种。

[0045] 需要说明，上述“若干特定隐私行为”中的“若干”，以及文中记载的其他处“若干”，含义都是一个或多个，不包含0。

[0046] 用户对于其某些隐私行为，例如，一些个人比较私密的行为习惯，是不希望被终端分析获知的，如，抽烟行为，半夜的进食行为等。在一个实施例中，上述若干特定隐私行为包括用户设定的禁止采集的行为和用户未授权采集的行为。在另一个实施例中，上述若干特定隐私行为可以是工作人员根据相关调查问卷的反馈进行分析而设定的。需要理解，上述业务预测任务中不会包括针对上述特定隐私行为的预测任务。

[0047] 对于上述若干特定隐私行为中任一的第一隐私行为(其中“第一”仅用于区分同类事物，不具有其他排序等限定作用)，原始数据记录中包含可以判定用户是否做出该第一隐私行为的传感器数据，该传感器数据可以是一条或多条原始传感器数据。需要理解，特定隐私行为与传感器之间的映射关系(也就是哪几个传感器对应的原始采集数据可以反映用户是否做出某种特定隐私行为)，以及利用传感器数据判别用户是否做出特定隐私行为的判别方式(例如，采用阈值判别或模型判别)，都可以是预先确定好的。

[0048] 基于此，针对上述第一隐私行为，在一个实施例中，可以根据预先设定的传感器与特定隐私行为之间的映射关系，从上述多条原始传感器数据中确定与所述第一隐私行为对应的若干条第一原始数据，并基于该若干条第一原始数据，判断用户是否做出所述第一隐私行为；进一步地，一方面，在判断出用户做出第一隐私行为的情况下，将该若干条第一原始数据归入若干条敏感传感器数据中；另一方面，在判断出用户未做出第一隐私行为的情况下，不将该若干条第一原始数据判定为敏感传感器数据。

[0049] 在一个具体的实施例中，上述基于若干条第一原始数据，判断用户是否做出所述第一隐私行为，可以包括：将该若干条第一原始数据输入预先训练的第一行为预测模型中，得到预测结果，指示用户是否做出该第一隐私行为。在一个例子中，假定上述若干隐私行为中包括抽烟行为，根据上述映射关系可以确定出与该抽烟行为对应的传感器包括重力传感器和心率传感器，进而获取重力传感器数据和心率传感器数据，输入抽烟行为预测模型中，得到指示用户是否进行抽烟的预测结果。进一步地，如果该预测结果指示用户在抽烟，则将重力传感器数据和心率传感器数据归入若干条敏感传感器数据中，否则不进行其他处理。需要说明，第一行为预测模型的使用过程和训练过程类似，区别主要在于训练过程用到样本标签进行模型调参，故而在此不对训练过程进行赘述。

[0050] 在另一个具体的实施例中，上述基于若干条第一原始数据，判断用户是否做出所述第一隐私行为，可以包括：首先，判断其中各条第一原始数据是否在各自对应的预设区间内；然后，在判断出均在各自对应的预设区间内的情况下，判定用户做出所述第一隐私行为。在一个例子中，假定上述若干隐私行为中包括心率偏高(仅作为示例性说明)，则其对应的预设区间可以为(120，200)，此时，根据上述映射关系可以确定出于该心率偏高对应的传感器是心率传感器，进而获取心率传感器数据，在判断出该心率传感器数据落入对应预设区间的情况下，判定用户心率偏高，并将该心率传感器数据归入若干条敏感传感器数据中。如此，可以实现对原始数据记录中是否存在敏感传感器数据的判定。

[0051] 需要说明，可能存在某条原始传感器数据跟多个特定隐私行为相关的情况，此时，

只要根据该某条原始传感器数据可以判定出做出该多个特定隐私行为中的某一个特定隐私行为，则将其归入敏感传感器数据。

[0052] 以上，可以实现对原始数据记录中是否包含敏感传感器数据的判断。进一步地，一方面，在判断出其中包括若干条敏感传感器数据的情况下，执行后续步骤。另一方面，在判断出其中不包括任何敏感传感器数据的情况下，可以终止当前流程。

[0053] 在步骤S230，在判断出包含若干条敏感传感器数据的情况下，利用中性数据(非敏感数据)对原始数据记录中的该若干条敏感传感器数据进行替换，得到脱敏数据记录。

[0054] 需要说明，针对上述特定隐私行为和传感器之间的映射关系，对于该映射关系中涉及的一个或多个传感器，可以预先确定与其中每一个传感器对应的一条脱敏传感器数据。基于此，对于上述若干条敏感传感器数据对应的若干传感器，可以获取与该若干个传感器对应的若干条脱敏传感器数据，对原始数据记录中的上述若干条敏感传感器数据进行替换，得到脱敏数据记录。

[0055] 对于上述脱敏传感器数据的确定，在一个实施例中，针对与第一传感器对应的第一脱敏传感器数据，可以先获取多个用户终端中多个第一传感器采集得到的多条第一原始传感器数据，再对该多条第一原始传感器数据进行平均处理，并将平均处理的结果作为上述第一脱敏传感器数据。需要理解，通过平均处理得到的脱敏传感器数据磨灭了不同用户的个人特性，因此得到的脱敏传感器数据是中性的。在另一个实施例中，还可以获取一些原始数据记录，其中每个原始数据记录均反映对应用户未做出上述若干特定隐私行为，此时，可以通过随机挑选或平均处理，得到与各个传感器对应的脱敏传感器数据，进而按需选用。

[0056] 以上，可以得到与原始数据记录对应的脱敏数据记录。在执行步骤S230的同时，之前或之后，可以执行步骤S240，将该原始数据记录输入数据脱敏模型，得到脱敏处理结果。在一个实施例中，其中数据脱敏模型可以基于深度神经网络(Deep Neural Networks，简称DNN)或卷积神经网络(Convolutional Neural Networks，简称CNN)等实现。在另一个实施例中，其中数据脱敏模型可以实现为自编码器(autoencoder，简称AE)。需要理解，原始数据记录和脱敏处理结果具有相同的数据格式，比如说，如果原始数据记录中包括M(M为大于1的整数)条原始传感器数据，其中各条原始传感器数据中包括W(W为大于1的整数)个数值，那么，脱敏处理结果中同样包括M条脱敏处理后传感器数据，其中各条脱敏处理后数据中包括的数值个数也为W。

[0057] 在以上得到数据脱敏模型输出的脱敏处理结果后，一方面，在步骤S250，基于该脱敏处理结果和上述脱敏数据记录，确定脱敏处理损失。需要理解，因脱敏数据记录和原始数据记录具有相同的数据格式，脱敏处理结果也和原始数据记录具有相同的数据格式，所以相应地，脱敏数据记录和脱敏处理结果具有相同的数据格式。在一个实施例中，可以计算脱敏处理结果和上述脱敏数据记录之间欧式距离、曼哈顿距离、余弦距离等，作为脱敏处理损失。如此，可以得到脱敏处理损失。

[0058] 另一方面，在步骤S260，将该脱敏处理结果输入预先训练的业务预测模型中，得到业务预测结果，该业务预测模型用于执行上述业务预测任务，进而在步骤S270，基于该业务预测结果和上述业务标签，确定业务预测损失。

[0059] 在一个实施例中，其中业务预测模型可以基于上述DNN网络或CNN网络等神经网络实现。在一个实施例中，在业务预测模型用于执行的业务预测任务为多项，相应在步骤S210

中获取的业务标签为多个的情况下，业务预测模型可以为多任务模型。在一个具体的实施例中，业务预测模型可以为由多个子模型集成得到的模型，其中一个子模型对应一项预测任务。

[0060] 在一个实施例中，上述业务预测模型可以基于多条原始数据记录和对应的多个业务标签进行预先训练而得到，如此得到的业务预测模型可以根据输入的原始数据记录输出准确的业务预测结果。需要说明，一方面，训练业务预测模型采用的训练方式可以采用现有的监督学习的方式实现，不作赘述。另一方面，本说明书一个或多个实施例披露的数据处理方法，旨在防止传感器数据泄露用户做出隐私行为，但同时，还要保证传感器数据可以良好地完成业务预测任务，因此希望，脱敏后的传感器数据在输入用针对原始传感器数据的打标数据进行训练得到的业务预测模型时，可以得到准确的预测结果，如此，可以使得后续多个应用APP等拿到利用训练好的数据脱敏模型输出的脱敏后的传感器数据时，仍然可以利用各自根据原始传感器数据训练好的机器学习模型，完成准确的业务预测。

[0061] 在一个实施例中，可以将上述脱敏处理结果直接输入上述业务预测模型中，得到业务预测结果。在另一个实施例中，还可以基于预先获取的上述业务预测任务与若干传感器之间的对应关系，从上述脱敏处理结果中获取与该若干传感器对应的若干条脱敏传感器数据，再将该若干条脱敏传感器数据输入上述业务预测模型中，得到业务预测结果。

[0062] 在一个实施例中，基于上述业务预测结果和业务标签，可以采用计算交叉熵损失或铰链损失等损失计算方式，确定上述业务预测损失。如此，可以得到业务预测损失。

[0063] 在以上确定出脱敏处理损失和业务预测损失之后，接着在步骤S280，基于该脱敏处理损失和业务预测损失，训练该数据脱敏模型。具体地，可以利用以下公式计算综合损失，再利用综合损失训练该数据脱敏模型。

[0064] $$L = \beta_1 L_1 + \beta_2 L_2 \quad (1)$$

[0065] 式(1)中，L表示综合损失；L_1和L_2分别表示上述脱敏处理损失和业务预测损失；β_1和β_2为超参数，均大于0，例如，可以设定二者分别为0.3和0.7。

[0066] 需要说明，其中的训练的具体方式可以采用现有技术实现，例如，可以利用反向传播法，调整数据脱敏模型中的参数，具体不作赘述。

[0067] 如此，通过重复执行上述步骤S210至步骤S280，可以实现对数据脱敏模型的多次迭代训练，直到迭代停止，可以将最后一次迭代后得到的数据脱敏模型作为最终使用的数据脱敏模型。其中迭代停止可以是迭代至预定次数，或者，迭代至模型性能达到预设标准。

[0068] 上述最终使用的数据脱敏模型可用于对目标原始数据记录进行脱敏处理，脱敏处理后得到的传感器数据，可以被用于提供给用户终端的应用APP，或者，其他经用户授权的使用平台。

[0069] 综上，采用本说明书实施例披露的实现隐私保护的数据处理方法，可以实现对原始传感器数据的脱敏处理，从而防止用户隐私行为的泄露，保障用户隐私安全，同时，保证脱敏处理后的传感器数据，可以被正常用于相关业务的处理，在业务处理中具有足够高的可用性。

[0070] 上述披露的数据处理方法中，主要是防止泄露用户做出某些隐私行为。实际上，除了隐私行为以外，用户还可能希望，自己是否做出(包括是和否)隐私行为都不被泄露，以及

一些自身的隐私属性(如性别、年龄)等也不被泄露。由此,本说明书还披露一种实现隐私保护的数据处理方法,可以有效防止用户隐私信息的泄露,其隐私信息可以包括上述特定隐私行为。

[0071] 为便于理解,图3示出根据另一个实施例的数据脱敏模型的训练实施架构图,如图3所示,对于用户终端中包括的多个传感器(图1中示出N个,N为大于1的整数),各个传感器各自进行数据采集,对应得到N条原始传感器数据,基于此,可以获取该N条原始传感器数据,构成原始数据记录;接着,基于预先确定的与若干传感器对应的若干条脱敏传感器数据,对所述原始数据记录中与所述若干传感器对应的若干条原始传感器数据进行替换,得到脱敏数据记录,其中若干传感器采集的原始数据可用于推断用户的特定隐私信息;然后,将原始数据记录输入数据脱敏模型中,得到脱敏处理结果;接着,一方面,基于脱敏处理结果和脱敏数据记录确定脱敏处理损失,另一方面,将脱敏处理结果输入预先训练的业务预测模型中,得到业务预测结果(例如,跑步模式),并基于业务预测结果和与原始数据记录对应的业务标签,确定业务预测损失;进一步地,基于脱敏处理损失和业务预测损失,训练上述数据脱敏模型。如此,可以实现对数据脱敏处理模型的训练。

[0072] 下面,描述上述数据处理方法的具体实施步骤。

[0073] 图4示出根据另一个实施例的实现隐私保护的数据处理方法的流程示意图,所述方法的执行主体可以为任何具有计算、处理能力的装置或平台或设备集群。如图4所示,所述方法包括以下步骤:

[0074] 步骤S410,获取原始数据记录和对应的业务标签;该原始数据记录中包括多条原始传感器数据,其由用户终端中的多个传感器进行采集而得到;该业务标签对应针对用户的业务预测任务;步骤S420,获取预先确定的与若干传感器对应的若干条脱敏传感器数据,其中若干传感器采集的原始数据可用于推断用户的特定隐私信息;步骤S430,利用该若干条脱敏传感器数据,对该原始数据记录中与该若干传感器对应的若干条原始传感器数据进行替换,得到脱敏数据记录;步骤S440,将该原始数据记录输入数据脱敏模型,得到脱敏处理结果;步骤S450,基于该脱敏处理结果和该脱敏数据记录,确定脱敏处理损失;步骤S460,将该脱敏处理结果输入预先训练的业务预测模型中,得到业务预测结果,该业务预测模型用于执行该业务预测任务;步骤S470,基于该业务预测结果和该业务标签,确定业务预测损失;步骤S480,基于该第一脱敏处理损失和业务预测损失,训练该数据脱敏模型;训练后的数据脱敏模型用于对目标原始数据记录进行脱敏处理。

[0075] 针对以上步骤,需要说明的是,相较于图3中示出的方法,主要的不同在于步骤S420和步骤S430,与上述步骤S320和步骤S330之间的不同,在步骤S320和步骤S330中,是先对原始数据记录中是否包含反映用户做出特定隐私行为的敏感传感器数据进行判断,在判断出包含的情况下再进行对应的替换,从而得到脱敏数据记录,而在步骤S420和步骤S430中,不需要进行任何判断,而是直接对可以推断出特定敏感信息(可以包括上述特定隐私行为)的传感器数据全部进行替换,从而得到脱敏数据记录。通过图4示出的数据处理方法训练出的数据处理模型,不但可以用于防止用户做出特定隐私行为被泄露,还可以防止用户未做出特定隐私行为被泄露,也就是无从判断用户是否做出特定隐私行为,以及,还可以防止特定隐私行为以外的隐私属性(如性别、年龄、身高等)被泄露。

[0076] 此外,对于上述图4中步骤的描述,可以参见前述实施例中对图3示出的方法步骤

的描述，在此不作赘述。

[0077] 综上，采用本说明书实施例披露的实现隐私保护的数据处理方法，可以实现对原始传感器数据的脱敏处理，从而防止用户隐私信息的泄露，保障用户隐私安全，同时，保证脱敏处理后的传感器数据，可以被正常用于相关业务的处理，在业务处理中具有足够高的可用性。

[0078] 与上述数据处理方法相对应的，本说明书实施例还披露数据处理装置。具体如下：

[0079] 图5示出根据一个实施例的实现隐私保护的数据处理方装置的结构图，如图5所示，所述装置500包括：

[0080] 获取单元510，配置为获取原始数据记录和对应的业务标签；上述原始数据记录中包括多条原始传感器数据，其由用户终端中的多个传感器进行采集而得到；上述业务标签对应针对用户的业务预测任务；判断单元520，配置为判断上述原始数据记录中是否包含敏感传感器数据，该敏感传感器数据反映用户做出若干特定隐私行为中的至少一种；替换单元530，配置为在判断出包含若干条敏感传感器数据的情况下，利用预先确定的若干条脱敏传感器数据，替换上述原始数据记录中的上述若干条敏感传感器数据，得到脱敏数据记录，其中若干条敏感传感器数据和若干条脱敏传感器数据对应相同的若干个传感器；脱敏单元540，配置为将上述原始数据记录输入数据脱敏模型，得到脱敏处理结果；脱敏损失确定单元550，配置为基于上述脱敏处理结果和上述脱敏数据记录，确定脱敏处理损失；业务预测单元560，配置为将上述脱敏处理结果输入预先训练的业务预测模型中，得到业务预测结果，上述业务预测模型用于执行上述业务预测任务；业务损失确定单元570，配置为基于上述业务预测结果和上述业务标签，确定业务预测损失；模型训练单元580，配置为基于上述脱敏处理损失和业务预测损失，训练上述数据脱敏模型；训练后的数据脱敏模型用于对目标原始数据记录进行脱敏处理。

[0081] 在一个实施例中，其中各条原始传感器数据包括观测值序列，该观测值序列由传感器在多个预定时刻采集到的多个观测值组成。

[0082] 在一个实施例中，上述多个传感器中包括以下中的至少一个：重力传感器，位置传感器，加速度传感器，角速度传感器，心率传感器。

[0083] 在一个实施例中，上述若干特定隐私行为包括用户设定的禁止采集的行为和/或用户未授权采集的行为，上述业务预测任务对应用户授权的业务。

[0084] 在一个实施例中，上述若干特定隐私行为中包括第一隐私行为；上述判断单元520具体包括：确定子单元521，配置为基于预先设定的传感器与特定隐私行为之间的映射关系，从上述多条原始传感器数据中确定与上述第一隐私行为对应的若干条第一原始数据；判断子单元522，配置为基于上述若干条第一原始数据，判断用户是否做出上述第一隐私行为；归入子单元523，配置为在判断出用户做出上述第一隐私行为的情况下，将上述若干条第一原始数据归入上述若干条敏感传感器数据中。

[0085] 在一个具体的实施例中，上述判断子单元522具体配置为：将上述若干条第一原始数据输入预先训练的第一行为预测模型中，得到预测结果，指示用户是否做出上述第一隐私行为。

[0086] 在另一个具体的实施例中，上述判断子单元522具体配置为：判断其中各条第一原始数据是否在各自对应的预设区间内；在判断出均在各自对应的预设区间内的情况下，判

定用户做出上述第一隐私行为。

[0087] 在一个实施例中，上述若干条脱敏传感器数据中包括对应于第一传感器的第一脱敏传感器数据，其基于数据确定单元而得到，上述数据确定单元配置为：获取多条第一原始传感器数据，其由多个用户终端中的多个第一传感器采集得到；对上述多条第一原始传感器数据进行平均处理，得到上述第一脱敏传感器数据。

[0088] 在一个实施例中，上述业务预测模型基于多条原始数据记录和对应的多个业务标签进行预先训练而得到。

[0089] 综上，采用本说明书实施例披露的实现隐私保护的数据处理装置，可以实现对原始传感器数据的脱敏处理，从而防止用户隐私行为的泄露，保障用户隐私安全，同时，保证脱敏处理后的传感器数据，可以被正常用于相关业务的处理，在业务处理中具有足够高的可用性。

[0090] 图6示出根据另一个实施例的实现隐私保护的数据处理方装置的结构图，如图6所示，所述装置600包括：

[0091] 第一获取单元610，配置为获取原始数据记录和对应的业务标签；上述原始数据记录中包括多条原始传感器数据，其由用户终端中的多个传感器进行采集而得到；上述业务标签对应针对用户的业务预测任务；第二获取单元620，配置为获取预先确定的与若干传感器对应的若干条脱敏传感器数据，其中若干传感器采集的原始数据可用于推断用户的特定隐私信息；替换单元630，配置为利用上述若干条脱敏传感器数据，对上述原始数据记录中与上述若干传感器对应的若干条原始传感器数据进行替换，得到脱敏数据记录；脱敏单元640，配置为将上述原始数据记录输入数据脱敏模型，得到脱敏处理结果；脱敏损失确定单元650，配置为基于上述脱敏处理结果和上述脱敏数据记录，确定脱敏处理损失；业务预测单元660，配置为将上述脱敏处理结果输入预先训练的业务预测模型中，得到业务预测结果，上述业务预测模型用于执行上述业务预测任务；业务损失确定单元670，配置为基于上述业务预测结果和上述业务标签，确定业务预测损失；模型训练单元680，配置为基于上述第一脱敏处理损失和业务预测损失，训练上述数据脱敏模型；训练后的数据脱敏模型用于对目标原始数据记录进行脱敏处理。

[0092] 在一个实施例中，上述特定隐私信息包括性别和/或年龄。

[0093] 综上，采用本说明书实施例披露的实现隐私保护的数据处理装置，可以实现对原始传感器数据的脱敏处理，从而防止用户隐私信息的泄露，保障用户隐私安全，同时，保证脱敏处理后的传感器数据，可以被正常用于相关业务的处理，在业务处理中具有足够高的可用性。

[0094] 根据另一方面的实施例，还提供一种计算机可读存储介质，其上存储有计算机程序，当上述计算机程序在计算机中执行时，令计算机执行结合图2所描述的方法。

[0095] 根据再一方面的实施例，还提供一种计算设备，包括存储器和处理器，上述存储器中存储有可执行代码，上述处理器执行上述可执行代码时，实现结合图2所描述的方法。

[0096] 本领域技术人员应该可以意识到，在上述一个或多个示例中，本发明所描述的功能可以用硬件、软件、固件或它们的任意组合来实现。当使用软件实现时，可以将这些功能存储在计算机可读介质中或者作为计算机可读介质上的一个或多个指令或代码进行传输。

[0097] 以上上述的具体实施方式，对本发明的目的、技术方案和有益效果进行了进一步

详细说明，所应理解的是，以上上述仅为本发明的具体实施方式而已，并不用于限定本发明的保护范围，凡在本发明的技术方案的基础之上，所做的任何修改、等同替换、改进等，均应包括在本发明的保护范围之内。

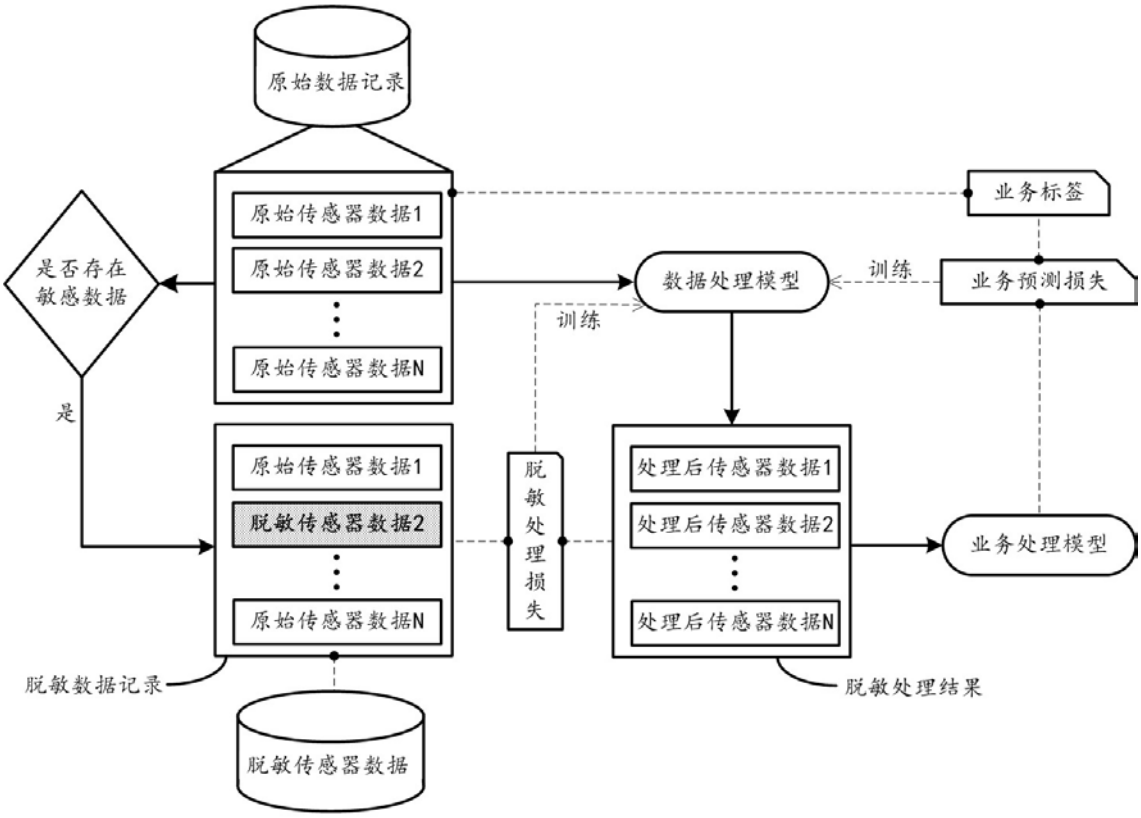

原始数据记录
原始传感器数据1
原始传感器数据2
原始传感器数据N
是否存在敏感数据
是
业务标签
数据处理模型
训练
业务预测损失
训练
原始传感器数据1
脱敏传感器数据2
原始传感器数据N
脱敏处理损失
处理后传感器数据1
处理后传感器数据2
处理后传感器数据N
业务处理模型
脱敏数据记录
脱敏传感器数据
脱敏处理结果

图1

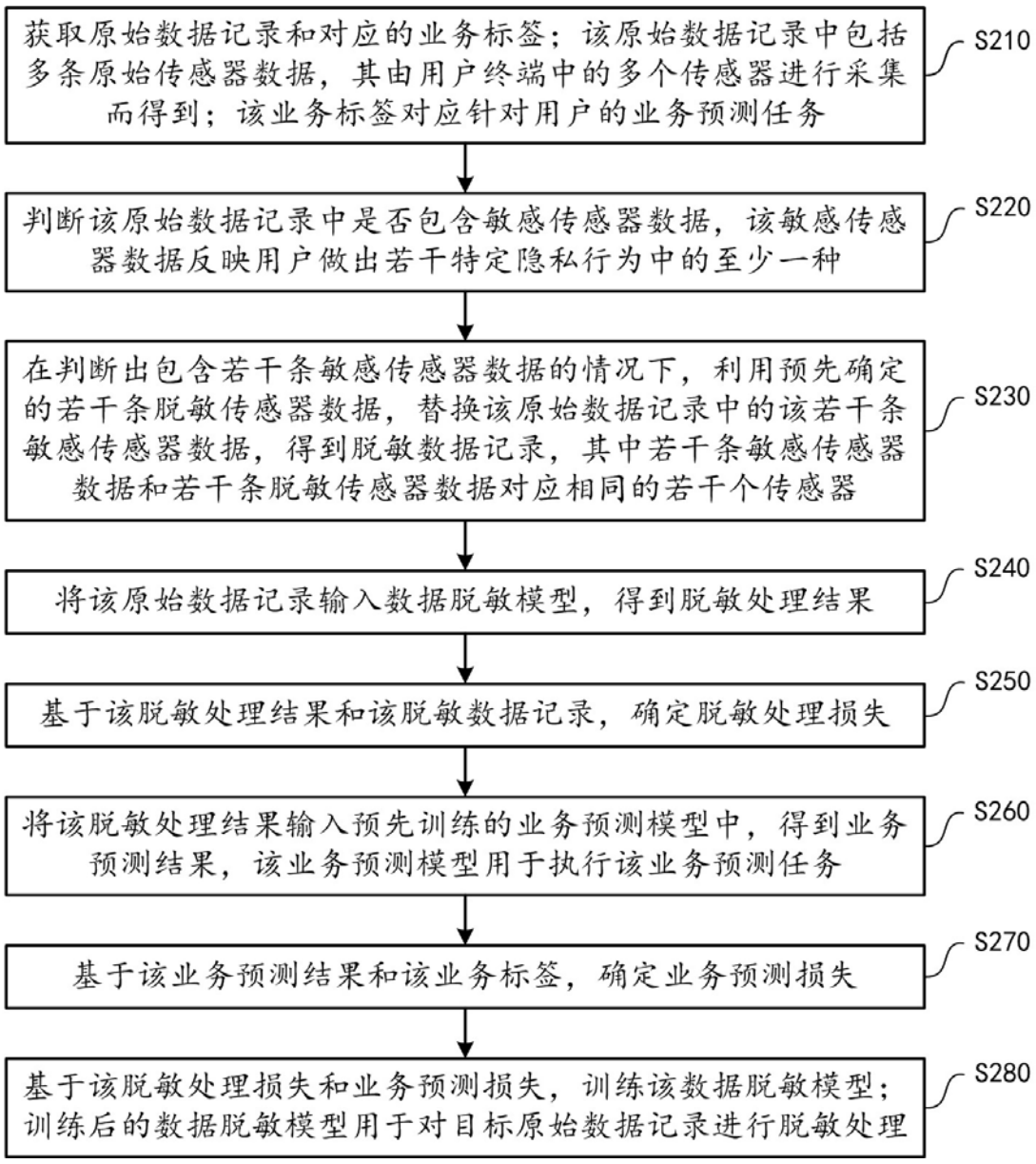

获取原始数据记录和对应的业务标签；该原始数据记录中包括多条原始传感器数据，其由用户终端中的多个传感器进行采集而得到；该业务标签对应针对用户的业务预测任务
S210
判断该原始数据记录中是否包含敏感传感器数据，该敏感传感器数据反映用户做出若干特定隐私行为中的至少一种
S220
在判断出包含若干条敏感传感器数据的情况下，利用预先确定的若干条脱敏传感器数据，替换该原始数据记录中的该若干条敏感传感器数据，得到脱敏数据记录，其中若干条敏感传感器数据和若干条脱敏传感器数据对应相同的若干个传感器
S230
将该原始数据记录输入数据脱敏模型，得到脱敏处理结果
S240
基于该脱敏处理结果和该脱敏数据记录，确定脱敏处理损失
S250
将该脱敏处理结果输入预先训练的业务预测模型中，得到业务预测结果，该业务预测模型用于执行该业务预测任务
S260
基于该业务预测结果和该业务标签，确定业务预测损失
S270
基于该脱敏处理损失和业务预测损失，训练该数据脱敏模型；训练后的数据脱敏模型用于对目标原始数据记录进行脱敏处理
S280

图2

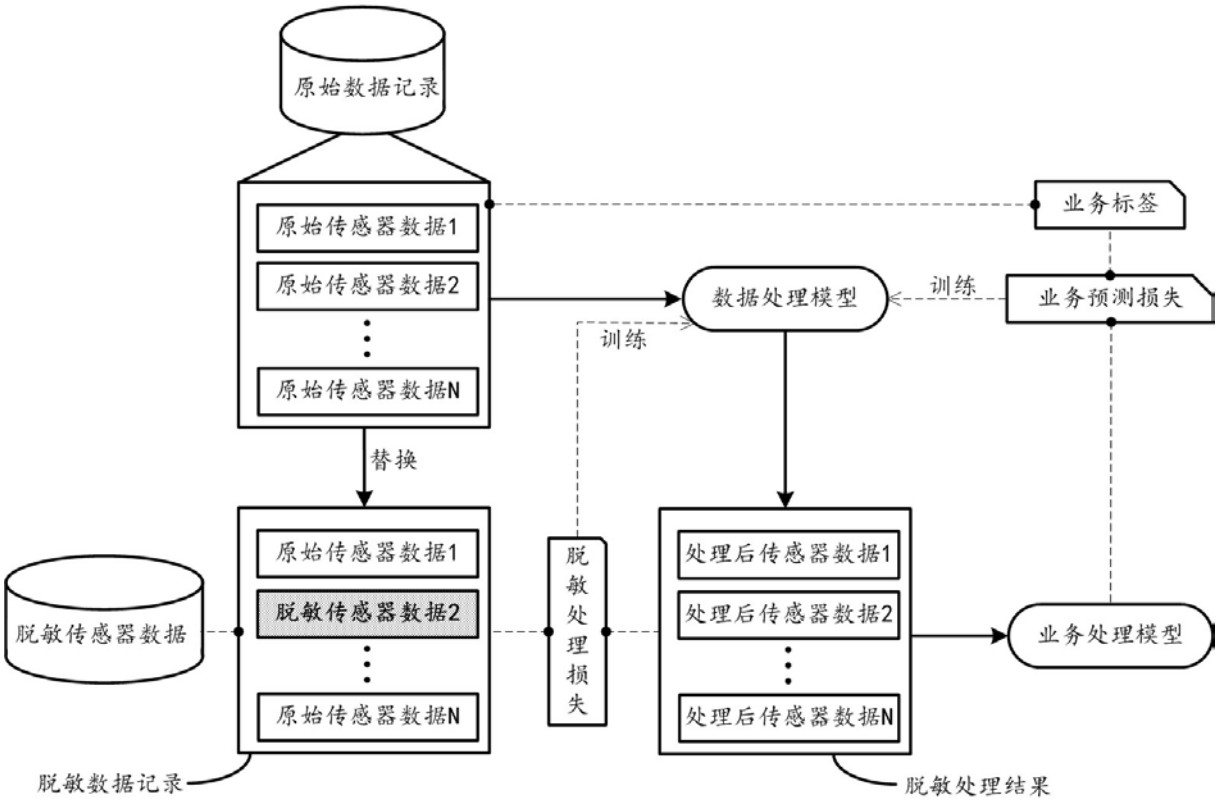

原始数据记录
原始传感器数据1
原始传感器数据2
原始传感器数据N
业务标签
数据处理模型
训练
业务预测损失
训练
替换
脱敏传感器数据
原始传感器数据1
脱敏传感器数据2
原始传感器数据N
脱敏处理损失
处理后传感器数据1
处理后传感器数据2
处理后传感器数据N
业务处理模型
脱敏数据记录
脱敏处理结果

图3

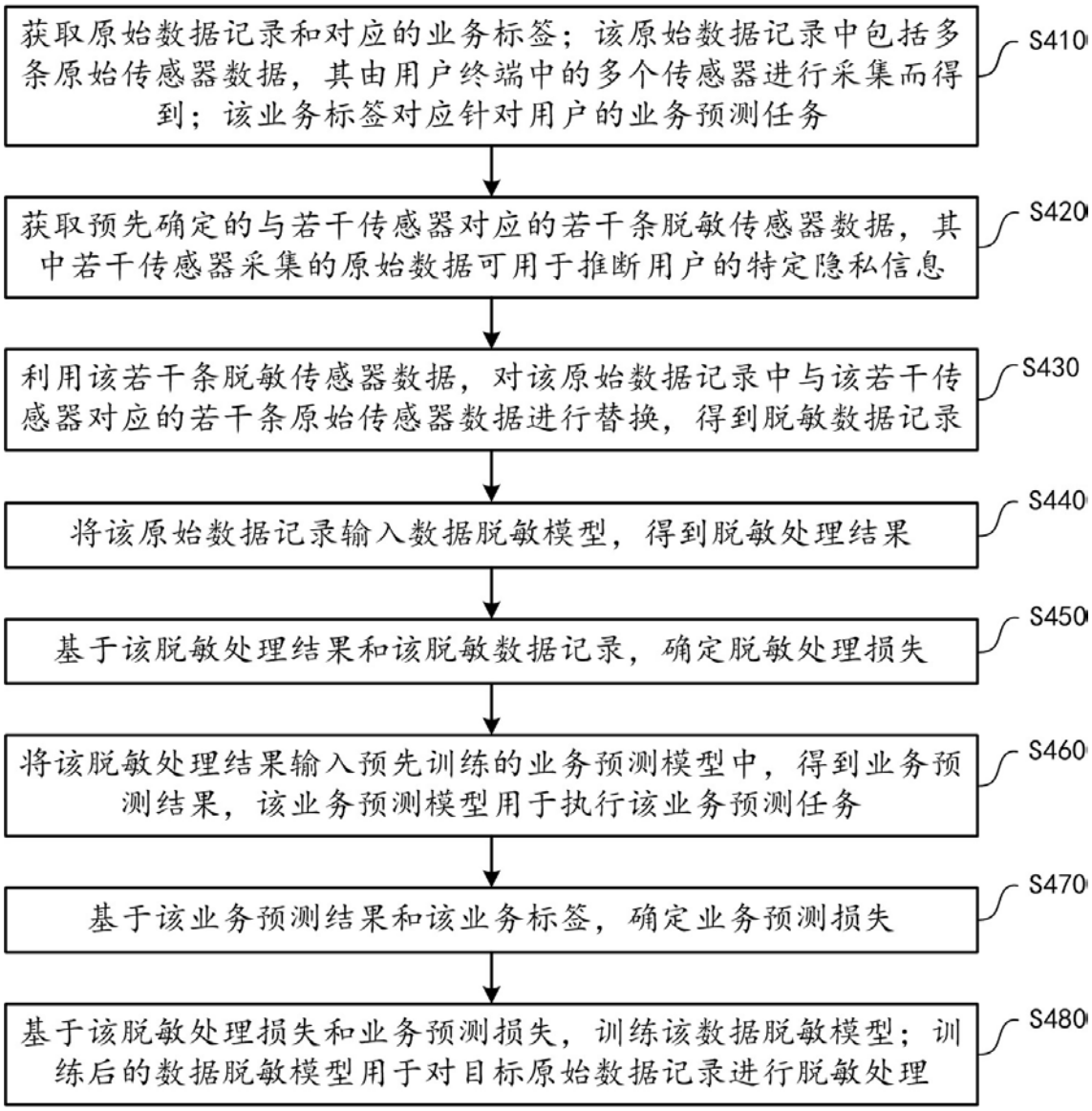

获取原始数据记录和对应的业务标签；该原始数据记录中包括多条原始传感器数据，其由用户终端中的多个传感器进行采集而得到；该业务标签对应针对用户的业务预测任务
S410
获取预先确定的与若干传感器对应的若干条脱敏传感器数据，其中若干传感器采集的原始数据可用于推断用户的特定隐私信息
S420
利用该若干条脱敏传感器数据，对该原始数据记录中与该若干传感器对应的若干条原始传感器数据进行替换，得到脱敏数据记录
S430
将该原始数据记录输入数据脱敏模型，得到脱敏处理结果
S440
基于该脱敏处理结果和该脱敏数据记录，确定脱敏处理损失
S450
将该脱敏处理结果输入预先训练的业务预测模型中，得到业务预测结果，该业务预测模型用于执行该业务预测任务
S460
基于该业务预测结果和该业务标签，确定业务预测损失
S470
基于该脱敏处理损失和业务预测损失，训练该数据脱敏模型；训练后的数据脱敏模型用于对目标原始数据记录进行脱敏处理
S480

图4

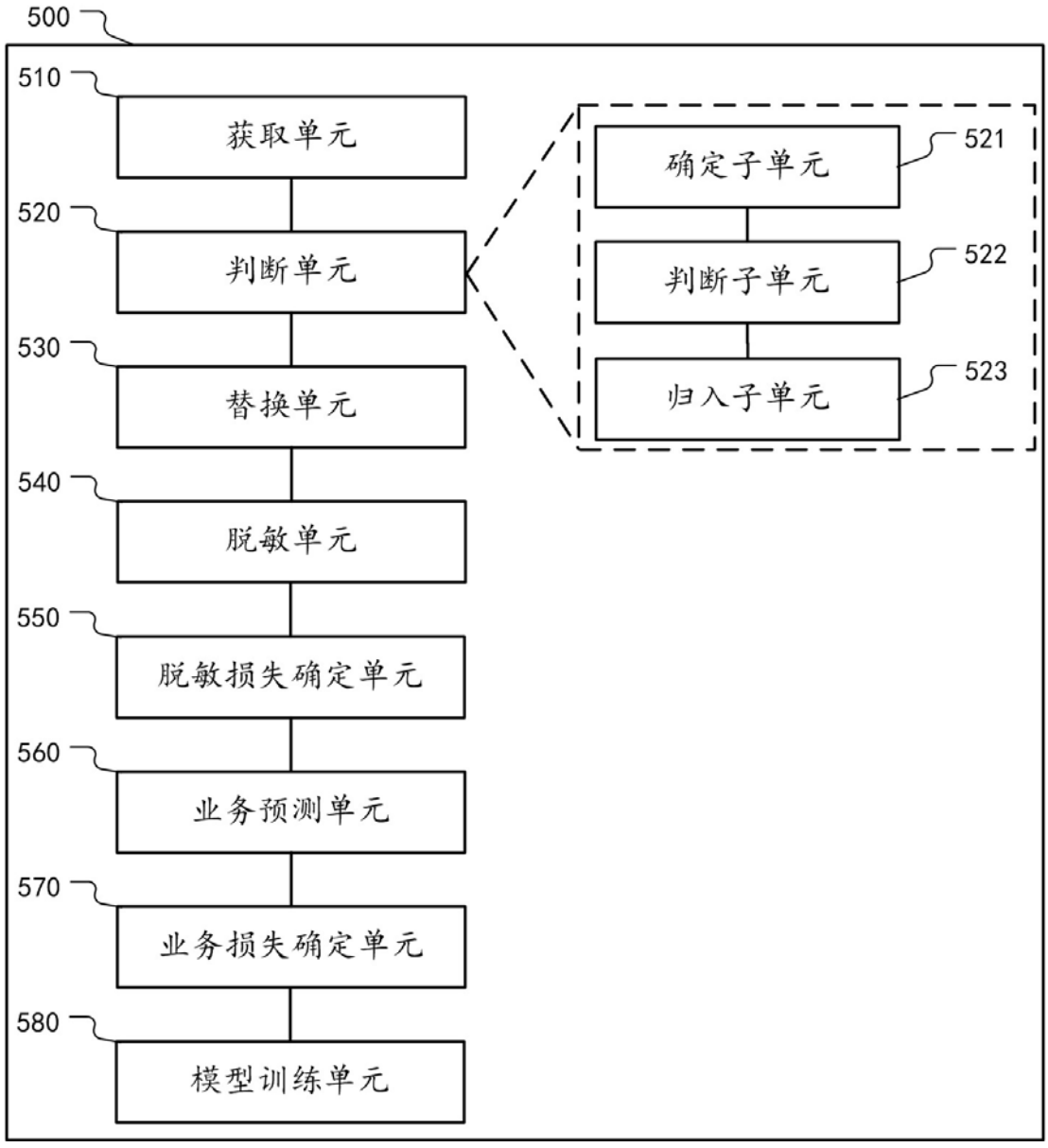

500
510
获取单元
520
判断单元
530
替换单元
540
脱敏单元
550
脱敏损失确定单元
560
业务预测单元
570
业务损失确定单元
580
模型训练单元
确定子单元
521
判断子单元
522
归入子单元
523

图5

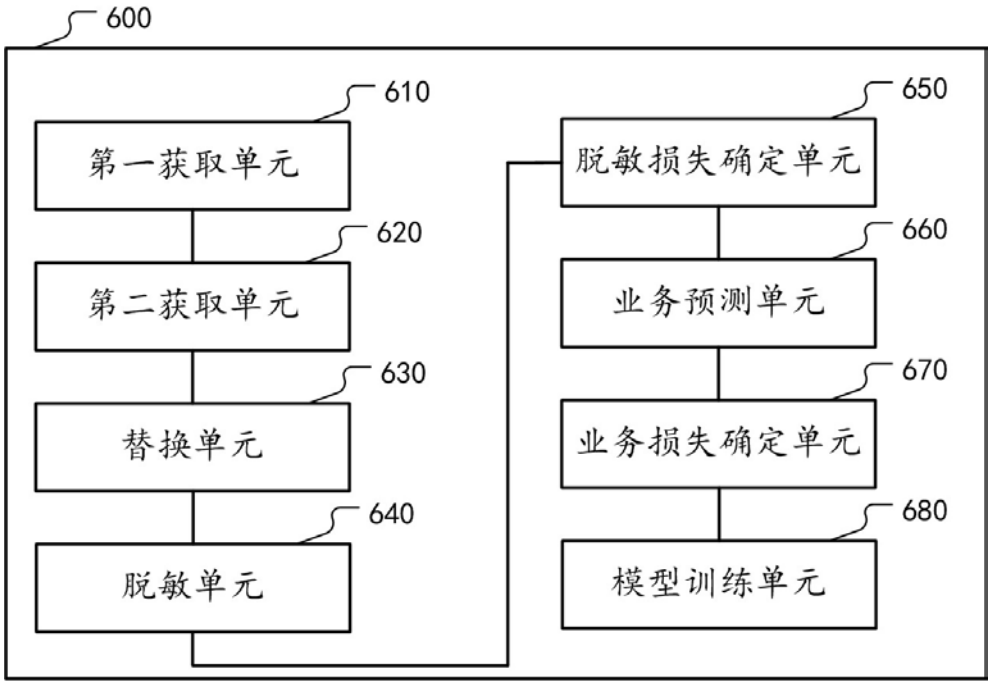

600
610
第一获取单元
620
第二获取单元
630
替换单元
640
脱敏单元
650
脱敏损失确定单元
660
业务预测单元
670
业务损失确定单元
680
模型训练单元

图6