

基于差分隐私的业务分析方法及装置

技术领域

[01] 本说明书一个或多个实施例涉及差分隐私技术领域，特别涉及一种基于差分隐私的业务分析方法及装置。

背景技术

[02] 大数据技术需要对人们在工作生活中产生的数据进行统计和分析，随着大数据技术的不断发展，人们的各种数据被采集，隐私问题也凸显出来。目前来说，一般采用差分隐私的方法对数据进行隐私保护的处理，但通常由于隐私预算太小，隐私保护过分严格，而导致数据中大部分有效信息被破坏，使得经过差分隐私处理的数据无法被用于业务分析中。

发明内容

[03] 为了解决上述技术问题之一，本说明书一个或多个实施例提供一种基于差分隐私的业务分析方法及装置。

[04] 根据第一方面，提供一种基于差分隐私的业务分析方法，所述方法包括至少一个业务分析阶段，任一个业务分析阶段包括至少一轮操作；该业务分析阶段的第 n 轮的操作包括以下步骤，其中， n 大于等于 1：获取目标数据；所述目标数据为对待处理数据进行匿名化处理得到的；所述待处理数据包括多个用户设备各自上传的各组差分隐私数据；任一组差分隐私数据由对应的用户设备利用第 n 轮的隐私预算，对该业务分析阶段中该用户设备的隐私数据进行差分隐私处理得到；对所述目标数据进行预设的业务分析；若所述业务分析成功，结束该业务分析阶段；若所述业务分析失败，确定第 $n+1$ 轮的隐私预算，并向所述多个用户设备发送所述第 $n+1$ 轮的隐私预算，使各个用户设备重新对该业务分析阶段中各自的隐私数据进行差分隐私处理，以进行第 $n+1$ 轮的操作。

[05] 可选的，所述确定第 $n+1$ 轮的隐私预算，包括：按照增大所述第 n 轮的隐私预算的方向确定候选隐私预算；判断所述候选隐私预算是否可用；若所述候选隐私预算可用，基于所述候选隐私预算确定所述第 $n+1$ 轮的隐私预算。

[06] 可选的，所述判断所述候选隐私预算是否可用，包括：确定该分析阶段已执行完成的各轮操作的隐私预算的总和；基于所述总和与所述候选隐私预算相加得到的结果，确定所述候选隐私预算是否可用。

[07] 可选的，所述差分隐私处理为 ϵ, δ -本地差分隐私处理；所述隐私预算包括 ϵ 本地隐私预算以及 δ 隐私预算；所述候选隐私预算包括 ϵ 候选全局隐私预算以及 δ 候选隐私预算；其中，所述确定候选隐私预算，包括：确定 ϵ 候选全局隐私预算以及 δ 候选隐私预算，使所述 ϵ 候选全局隐私预算大于当前存储的第 n 轮 ϵ 全局隐私预算，使所述 δ 候选隐私预算大于第 n 轮 δ 隐私预算；其中，所述判断所述候选隐私预算是否可用，包括：判断所述 ϵ 候选全局隐私预算以及所述 δ 候选隐私预算是否可用；其中，所述若所述候选隐私预算可用，基于所述候选隐私预算确定所述第 $n+1$ 轮的隐私预算，包括：若所述 ϵ 候选全局隐私预算以及所述 δ 候选隐私预算可用，基于所述 ϵ 候选全局隐私预算以及所述 δ 候选隐私预算，确定用于所述用户设备的第 $n+1$ 轮的 ϵ 本地隐私预算，并将所述 ϵ 候选全局隐私预算存储为第 $n+1$ 轮的 ϵ 全局隐私预算；将 δ 候选隐私预算作为第 $n+1$ 轮的 δ 隐私预算。

[08]可选的,所述判断所述 ϵ 候选全局隐私预算以及所述 δ 候选隐私预算是否可用,包括:确定该分析阶段已执行完成的各轮操作的 ϵ 全局隐私预算及所述 ϵ 候选全局隐私预算的加权和,将所述加权和与预设矫正项相加的结果作为第一结果;其中,所述预设矫正项与该分析阶段已执行完成的各轮操作的 ϵ 全局隐私预算及所述 ϵ 候选全局隐私预算的平方和正相关;确定该分析阶段已执行完成的各轮操作的 δ 隐私预算及所述 δ 候选隐私预算的总和,作为第二结果;若所述第一结果小于第一预设值,并且所述第二结果小于第二预设值,则确定所述 ϵ 候选全局隐私预算以及所述 δ 候选隐私预算可用。

[09]可选的,所述基于所述 ϵ 候选全局隐私预算以及所述 δ 候选隐私预算,确定用于所述用户设备的第 $n+1$ 轮的 ϵ 本地隐私预算,包括:基于所述 δ 候选隐私预算,确定目标系数;所述目标系数与所述 δ 候选隐私预算正相关;所述目标系数与所述多个用户设备的数目正相关;将所述 ϵ 候选全局隐私预算与所述目标系数相乘,得到所述第 $n+1$ 轮的 ϵ 本地隐私预算。

[10]可选的,所述获取目标数据,包括:在可信执行环境中获取所述待处理数据,并在所述可信执行环境中对所述待处理数据进行匿名化处理,得到所述目标数据。

[11]可选的,对所述目标数据进行预设的业务分析,包括:对所述目标数据进行统计分析;和/或对所述目标数据进行分类预测。

[12]可选的,任一个用户设备的隐私数据包括以下一项或多项:通过该用户设备输入的文本数据;通过该用户设备输入的表情符号;通过该用户设备点击链接的信息;在该用户设备上运行应用程序的信息;利用该用户设备收付款的信息;通过该用户设备浏览网页的信息;通过该用户设备搜索的信息;利用该用户设备播放音视频的信息;该用户设备的定位数据;利用该用户设备购买商品的信息。

[13]根据第二方面,提供一种基于差分隐私的业务分析装置,所述装置执行至少一个业务分析阶段,任一个业务分析阶段包括至少一轮操作;针对该业务分析阶段的第 n 轮的操作,其中, n 大于等于1,所述装置包括:获取模块,用于获取目标数据;所述目标数据为对待处理数据进行匿名化处理得到的;所述待处理数据包括多个用户设备各自上传的各组差分隐私数据;任一组差分隐私数据由对应的用户设备利用第 n 轮的隐私预算,对该业务分析阶段中该用户设备的隐私数据进行差分隐私处理得到;分析模块,用于对所述目标数据进行预设的业务分析;结束模块,用于在所述业务分析成功时,结束该业务分析阶段;确定模块,用于在所述业务分析失败时,确定第 $n+1$ 轮的隐私预算;发送模块,用于向所述多个用户设备发送所述第 $n+1$ 轮的隐私预算,使各个用户设备重新对该业务分析阶段中各自的隐私数据进行差分隐私处理,以进行第 $n+1$ 轮的操作。

[14]可选的,所述确定模块包括:第一确定子模块,用于按照增大所述第 n 轮的隐私预算的方向确定候选隐私预算;判断子模块,用于判断所述候选隐私预算是否可用;第二确定子模块,用于在所述候选隐私预算可用时,基于所述候选隐私预算确定所述第 $n+1$ 轮的隐私预算。

[15]可选的,所述判断子模块被配置用于:确定该分析阶段已执行完成的各轮操作的隐私预算的总和;基于所述总和与所述候选隐私预算相加得到的结果,确定所述候选隐私预算是否可用。

[16]可选的,所述差分隐私处理为 ϵ,δ -本地差分隐私处理;所述隐私预算包括 ϵ 本地隐私预算以及 δ 隐私预算;所述候选隐私预算包括 ϵ 候选全局隐私预算以及 δ 候选隐私预算;其中,所述第一确定子模块被配置用于:确定 ϵ 候选全局隐私预算以及 δ 候选隐私预算,使所述 ϵ 候选全局隐私预算大于当前存储的第 n 轮 ϵ 全局隐私预算,使所述 δ 候选隐私预算大于第 n 轮 δ 隐私预算;其中,所述判断子模块被配置用于:判断所述 ϵ 候

选全局隐私预算以及所述 δ 候选隐私预算是否可用；其中，所述第二确定子模块被配置用于：若所述 ϵ 候选全局隐私预算以及所述 δ 候选隐私预算可用，基于所述 ϵ 候选全局隐私预算以及所述 δ 候选隐私预算，确定用于所述用户设备的第 $n+1$ 轮的 ϵ 本地隐私预算，并将所述 ϵ 候选全局隐私预算存储为第 $n+1$ 轮的 ϵ 全局隐私预算；将 δ 候选隐私预算作为第 $n+1$ 轮的 δ 隐私预算。

[17]可选的，所述判断子模块通过如下方式判断所述 ϵ 候选全局隐私预算以及所述 δ 候选隐私预算是否可用：确定该分析阶段已执行完成的各轮操作的 ϵ 全局隐私预算及所述 ϵ 候选全局隐私预算的加权和，将所述加权和与预设矫正项相加的结果作为第一结果；其中，所述预设矫正项与该分析阶段已执行完成的各轮操作的 ϵ 全局隐私预算及所述 ϵ 候选全局隐私预算的平方和正相关；确定该分析阶段已执行完成的各轮操作的 δ 隐私预算及所述 δ 候选隐私预算的总和，作为第二结果；若所述第一结果小于第一预设值，并且所述第二结果小于第二预设值，则确定所述 ϵ 候选全局隐私预算以及所述 δ 候选隐私预算可用。

[18]可选的，所述第二确定子模块通过如下方式基于所述 ϵ 候选全局隐私预算以及所述 δ 候选隐私预算，确定用于所述用户设备的第 $n+1$ 轮的 ϵ 本地隐私预算：基于所述 δ 候选隐私预算，确定目标系数；所述目标系数与所述 δ 候选隐私预算正相关；所述目标系数与所述多个用户设备的数目正相关；将所述 ϵ 候选全局隐私预算与所述目标系数相乘，得到所述第 $n+1$ 轮的 ϵ 本地隐私预算。

[19]可选的，所述获取模块被配置用于：在可信执行环境中获取所述待处理数据，并在所述可信执行环境中对所述待处理数据进行匿名化处理，得到所述目标数据。

[20]可选的，所述分析模块被配置用于：对所述目标数据进行统计计算分析；和/或对所述目标数据进行分类预测。

[21]可选的，任一个用户设备的隐私数据包括以下一项或多项：通过该用户设备输入的文本数据；通过该用户设备输入的表情符号；通过该用户设备点击链接的信息；在该用户设备上运行应用程序的信息；利用该用户设备收付款的信息；通过该用户设备浏览网页的信息；通过该用户设备搜索的信息；利用该用户设备播放音视频的信息；该用户设备的定位数据；利用该用户设备购买商品的信息。

[22]根据第三方面，提供一种计算机可读存储介质，所述存储介质存储有计算机程序，所述计算机程序被处理器执行时实现上述第一方面中任一项所述的方法。

[23]根据第四方面，提供一种计算设备，包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序，所述处理器执行所述程序时实现上述第一方面中任一项所述的方法。

[24]本说明书的实施例提供的技术方案可以包括以下有益效果：本说明书的实施例提供的基于差分隐私的业务分析方法和装置，通过获取目标数据，对目标数据进行预设的业务分析，在该业务分析成功时，结束该业务分析阶段。在该业务分析失败时，确定第 $n+1$ 轮的隐私预算，并向该多个用户设备发送第 $n+1$ 轮的隐私预算，使各个用户设备重新对该业务分析阶段中各自的隐私数据进行差分隐私处理，以进行第 $n+1$ 轮的操作。从而能够在对数据进行差分隐私处理的过程中，自适应地调整隐私预算，增强了隐私保护过程的灵活性，提高了隐私保护数据的可用性。

[25]应当理解的是，以上的一般描述和后文的细节描述仅是示例性和解释性的，并不能限制本申请。

附图说明

[26] 为了更清楚地说明本申请实施例的技术方案，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申请的一些实施例，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。

[27] 图 1 是本说明书根据一示例性实施例示出的一种基于差分隐私的业务分析场景示意图；

[28] 图 2 是本说明书根据一示例性实施例示出的一种基于差分隐私的业务分析方法的流程图；

[29] 图 3 是本说明书根据一示例性实施例示出的另一种基于差分隐私的业务分析方法的流程图；

[30] 图 4 是本说明书根据一示例性实施例示出的另一种基于差分隐私的业务分析方法的流程图；

[31] 图 5 是本说明书根据一示例性实施例示出的一种基于差分隐私的业务分析装置的框图；

[32] 图 6 是本说明根据一示例性实施例示出的一种计算设备的结构示意图。

具体实施方式

[33] 这里将详细地对示例性实施例进行说明，其示例表示在附图中。下面的描述涉及附图时，除非另有表示，不同附图中的相同数字表示相同或相似的要素。以下示例性实施例中所描述的实施方式并不代表与本说明书相一致的所有实施方式。相反，它们仅是与如所附权利要求书中所详述的、本说明书的一些方面相一致的装置和方法的例子。

[34] 在本说明书中使用的术语是仅仅出于描述特定实施例的目的，而非旨在限制本申请。在本说明书和所附权利要求书中所使用的单数形式的“一种”、“所述”和“该”也旨在包括多数形式，除非上下文清楚地表示其他含义。还应当理解，本文中使用的术语“和/或”是指并包含一个或多个相关联的列出项目的任何或所有可能组合。

[35] 应当理解，尽管在本申请可能采用术语第一、第二、第三等来描述各种信息，但这些信息不应限于这些术语。这些术语仅用来将同一类型的信息彼此区分开。例如，在不脱离本申请范围的情况下，第一信息也可以被称为第二信息，类似地，第二信息也可以被称为第一信息。取决于语境，如在此所使用的词语“如果”可以被解释成为“在……时”或“当……时”或“响应于确定”。

[36] 如图 1 所示，是根据一示例性实施例示出的一种基于差分隐私的业务分析场景示意图。

[37] 参照图 1 示出的场景，在一个业务阶段第 n 轮的操作中 ($n \geq 1$)，多个用户设备各自确定该业务分析阶段中各自的隐私数据。并且，获取该业务分析阶段第 n 轮的隐私预算，基于该第 n 轮的隐私预算对该业务分析阶段中各自的隐私数据进行差分隐私处理，得到各自的一组差分隐私数据。然后，各个用户设备各自将各组差分隐私数据上传至云端平台。

[38] 云端平台在可信执行环境中接收各个用户设备各自上传的各组差分隐私数据，得到待处理数据。并在该可信执行环境中，对待处理数据进行匿名化处理，得到目标数据。

[39]接着，云端平台对目标数据进行业务分析，如果业务分析成功，可以输出业务分析的结果，并结束该业务分析阶段。如果业务分析失败，可以进一步确定该业务分析阶段第 $n+1$ 轮的隐私预算，并分别向该多个用户设备发送该第 $n+1$ 轮的隐私预算。使各个用户设备重新对该业务分析阶段中各自的隐私数据进行差分隐私处理，以进行该业务分析阶段第 $n+1$ 轮的操作，直至该业务分析阶段结束。

[40]下面将结合具体的实施例对本说明书提供的方案进行详细描述。

[41]如图 2 所示，图 2 是根据一示例性实施例示出的一种基于差分隐私的业务分析方法的流程图，该方法可以应用于云端平台中。云端平台可以实现为任何具有计算、处理能力的设备、平台、服务器或设备集群。该方法可以包括至少一个业务分析阶段，任一个业务分析阶段可以包括至少一轮操作。该业务分析阶段的第 n 轮 ($n \geq 1$) 的操作可以包括以下步骤：在步骤 201 中，获取目标数据。

[42]在本实施例中，目标数据为对待处理数据进行匿名化处理而得到的。其中，待处理数据可以包括多个用户设备各自上传的各组差分隐私数据，任一组差分隐私数据由对应的用户设备利用第 n 轮的隐私预算，对该业务分析阶段中该用户设备的隐私数据进行差分隐私处理得到。

[43]在一种实现方式中，云端平台部署有可信执行环境，在该可信执行环境中接收由多个用户设备各自上传的各组差分隐私数据，得到由各组差分隐私数据构成的待处理数据。并在该可信执行环境中对待处理数据进行匿名化处理，得到目标数据。

[44]在另一种实现方式中，多个用户设备可以各自将各组差分隐私数据上传至第三方平台的可信执行环境中。该第三方平台可以在可信执行环境中对由各组差分隐私数据构成的待处理数据进行匿名化处理，得到目标数据，并将目标数据传输至云端平台。

[45]在本实施例中，匿名化处理可以通过混淆机制进行的匿名化处理，本领域中已知的以及将来可能出现的任何匿名化处理的方法，都可以应用于本实施例中，本实施例对匿名化处理的具体方式方面不限定。

[46]在本实施例中，针对各个用户设备，在相同的业务分析阶段中，不同轮次处理相同的隐私数据。当一个业务分析阶段结束后，在下一个业务分析阶段，再换其它的隐私数据进行处理。

[47]其中，任意一个用户设备的隐私数据可以包括以下一项或多项：通过该用户设备输入的文本数据；通过该用户设备输入的表情符号；通过该用户设备点击链接的信息（例如，点击的链接的地址，点击链接的时刻等）；在该用户设备上运行应用程序的信息（例如，运行的应用程序的类型，运行的应用程序的时刻，运行的应用程序的时长等）；利用该用户设备收付款的信息（例如，收付款的类型，收付款的金额，收付款的时刻等）；通过该用户设备浏览网页的信息（例如，浏览的网页的类型，浏览的网页的时刻，浏览的网页的时长，浏览的网页中的关键字/词等）；通过该用户设备搜索的信息；利用该用户设备播放音视频的信息；该用户设备的定位数据；利用该用户设备购买商品的信息。可以理解，隐私数据还可以是其它类型的信息，本实施例对此方面不限定。

[48]在步骤 202 中，对目标数据进行预设的业务分析。

[49]在本实施例中，可以对目标数据进行预设的业务分析。具体来说，可以对目标数据进行统计计算分析，和/或对目标数据进行分类预测。例如，如果隐私数据为通过用户设备输入的文本数据，则预设的业务分析可以是统计计算某些预设短语的词频。又例如，如果隐私数据为收付款的信息和/或购买商品的信息，则预设的业务分析可以是统计消费群体的消费水平情况。又例如，如果隐私数据为用户搜索的信息，则预设的业务分析可

以是对社会热点问题的预测。再例如，如果隐私数据为定位数据，则预设的业务分析可以是对人群的分布与流动进行统计。

[50]可以理解，预设的业务分析还可以是其它类型的业务分析，本实施例对业务分析的具体类方面不限定。

[51]在步骤 203 中，若该业务分析成功，结束该业务分析阶段。

[52]在步骤 204 中，若该业务分析失败，确定第 $n+1$ 轮的隐私预算，并向该多个用户设备发送第 $n+1$ 轮的隐私预算，使各个用户设备重新对该业务分析阶段中各自的隐私数据进行差分隐私处理，以进行第 $n+1$ 轮的操作。

[53]在本实施例中，如果该业务分析可以得到结果，并且该结果满足预设要求，则说明该业务分析成功。如果该业务分析无法得到结果，或者可以得到结果，但得到的结果不满足预设要求，则说明该业务分析失败。

[54]在本实施例中，若上述业务分析成功，可以输出该业务分析的结果，并结束该业务分析阶段。若该业务分析失败，则可以确定第 $n+1$ 轮的隐私预算，并向该多个用户设备发送第 $n+1$ 轮的隐私预算。各个用户设备可以利用第 $n+1$ 轮的隐私预算，重新对该业务分析阶段中各自的隐私数据进行差分隐私处理，以进行第 $n+1$ 轮的操作。

[55]在一种实现方式中，可以按照预设的规则增大第 n 轮的隐私预算，作为第 $n+1$ 轮的隐私预算。例如，设第 n 轮的隐私预算为 ϵ ，则可以将第 n 轮的隐私预算增大 a ，得到第 $n+1$ 轮的隐私预算 $\epsilon+a$ 。

[56]在另一种实现方式中，还可以按照增大第 n 轮的隐私预算的方向确定候选隐私预算，判断候选隐私预算是否可用，在候选隐私预算可用时，基于候选隐私预算确定第 $n+1$ 轮的隐私预算。

[57]在本实施例中，可以采用 Renyi-差分隐私(Renyi Differential Privacy)的方法对隐私数据进行差分隐私处理，也可以采用 (ϵ, δ) -本地差分隐私的方法对隐私数据进行差分隐私处理，还可以采用 Concentrated-差分隐私 (Concentrated Differential Privacy)的方法对隐私数据进行差分隐私处理。可以理解，可以采用任意满足差分隐私协议的方法对隐私数据进行差分隐私处理，本实施例对差分隐私处理的具体类型方面不限定。

[58]在本实施例中，所涉及的隐私预算可以为差分隐私协议中的 ϵ ，或者是差分隐私协议中的 ϵ 和 δ 。需要说明的是，如果采用 (ϵ, δ) -本地差分隐私的方法对隐私数据进行差分隐私处理，该向用户设备发送的隐私预算为 ϵ 本地隐私预算以及 δ 隐私预算。其中，该 ϵ 本地隐私预算可以由 ϵ 全局隐私预算转换得到。

[59]本说明书的上述实施例提供的基于差分隐私的业务分析的方法，通过获取目标数据，对目标数据进行预设的业务分析，在该业务分析成功时，结束该业务分析阶段。在该业务分析失败时，确定第 $n+1$ 轮的隐私预算，并向该多个用户设备发送第 $n+1$ 轮的隐私预算，使各个用户设备重新对该业务分析阶段中各自的隐私数据进行差分隐私处理，以进行第 $n+1$ 轮的操作。从而能够在对数据进行差分隐私处理的过程中，自适应地调整隐私预算，增强了隐私保护过程的灵活性，提高了隐私保护数据的可用性。

[60]如图 3 所示，图 3 根据一示例性实施例示出的另一种基于差分隐私的业务分析方法的流程图，该实施例描述了确定第 $n+1$ 轮的隐私预算的过程，该方法可以应用于云端平台中，包括以下步骤：在步骤 301 中，获取目标数据。

[61]在本实施例中，目标数据为对待处理数据进行匿名化处理而得到的。其中，待处理数据可以包括多个用户设备各自上传的各组差分隐私数据，任一组差分隐私数据由对应的用户设备利用第 n 轮的隐私预算，对该业务分析阶段中该用户设备的隐私数据进行差

分隐私处理得到。

[62]在步骤 302 中, 对目标数据进行预设的业务分析。

[63]在本实施例中, 可以对目标数据进行预设的业务分析。具体来说, 可以对目标数据进行统计计算分析, 和/或对目标数据进行分类预测。

[64]在步骤 303 中, 若该业务分析成功, 结束该业务分析阶段。

[65]在步骤 304 中, 若该业务分析失败, 按照增大第 n 轮的隐私预算的方向确定候选隐私预算。

[66]在本实施例中, 可以采用任意满足差分隐私协议的方法对隐私数据进行差分隐私处理, 本实施例对差分隐私处理的具体类型方面不限定。隐私预算可以为差分隐私协议中的 ϵ , 或者也可以是差分隐私协议中的 ϵ 和 δ , 可以按照增大第 n 轮的隐私预算的方向确定候选隐私预算。

[67]在步骤 305 中, 判断该候选隐私预算是否可用。

[68]在步骤 306 中, 若该候选隐私预算可用, 基于该候选隐私预算确定第 $n+1$ 轮的隐私预算, 并向该多个用户设备发送第 $n+1$ 轮的隐私预算。

[69]在本实施例中, 若该候选隐私预算不可用, 可以适当调小该候选隐私预算, 并继续判断候选隐私预算是否可用。或者, 可以直接结束该业务分析阶段。若该候选隐私预算可用, 则可以基于该候选隐私预算确定第 $n+1$ 轮的隐私预算, 并向该多个用户设备发送第 $n+1$ 轮的隐私预算。

[70]具体来说, 可以通过任意合理的方式确定候选隐私预算, 判断该候选隐私预算是否可用, 并在该候选隐私预算可用时, 基于该候选隐私预算确定第 $n+1$ 轮的隐私预算。现举例如下: 在一种实现方式中, 如果采用除 (ϵ, δ) -本地差分隐私以外的一部分方法对隐私数据进行差分隐私处理, 该向用户设备发送的隐私预算包括 ϵ 隐私预算, 候选隐私预算包括 ϵ 候选隐私预算。则可以按照增大第 n 轮的 ϵ 隐私预算的方向, 确定 ϵ 候选隐私预算。例如, 第 n 轮的 ϵ 隐私预算为 ϵ_n , 那么, 候选隐私预算可以确定为 $\epsilon_n + \Delta_\epsilon$, 其中, $\Delta_\epsilon > 0$ 。

[71]然后, 可以确定该分析阶段已执行完成的各轮操作的 ϵ 隐私预算的总和, 并基于该总和与该 ϵ 候选隐私预算相加得到的结果, 确定该 ϵ 候选隐私预算是否可用。例如, 若该总和与该 ϵ 候选隐私预算相加得到的结果小于预设阈值, 则确定该 ϵ 候选隐私预算可用。若该总和与该 ϵ 候选隐私预算相加得到的结果大于等于预设阈值, 则确定该 ϵ 候选隐私预算不可用。

[72]最后, 若该 ϵ 候选隐私预算可用, 可以将该 ϵ 候选隐私预算作为第 $n+1$ 轮的 ϵ 隐私预算, 并向该多个用户设备发送第 $n+1$ 轮的 ϵ 隐私预算。例如, 第 n 轮的 ϵ 隐私预算为 ϵ_n , 候选隐私预算为 $\epsilon_n + \Delta_\epsilon$, 可以将 $\epsilon_n + \Delta_\epsilon$ 作为第 $n+1$ 轮的隐私预算, 即

$$\epsilon_{n+1} = \epsilon_n + \Delta_\epsilon。$$

[73]在另一种实现方式中, 如果采用除 (ϵ, δ) -本地差分隐私以外的另一部分方法对隐私数据进行差分隐私处理, 该向用户设备发送的隐私预算包括 ϵ 隐私预算和 δ 隐私预算, 候选隐私预算包括 ϵ 候选隐私预算以及 δ 候选隐私预算。可以按照增大第 n 轮的 ϵ 隐私预算的方向确定 ϵ 候选隐私预算, 以及按照增大第 n 轮的 δ 隐私预算的方向确定 δ 候选隐私预算。例如, 第 n 轮的隐私预算为 ϵ_n 和 δ_n , 候选隐私预算可以确定为 $\epsilon_n + \Delta_\epsilon$ 和 $\delta_n + \Delta_\delta$, 其中, $\Delta_\epsilon > 0$, $\Delta_\delta > 0$ 。

[74]然后, 可以确定该分析阶段已执行完成的各轮操作的 ϵ 隐私预算以及该 ϵ 候选隐私

预算相加的第一总和, 确定该分析阶段已执行完成的各轮操作的 δ 隐私预算以及该 δ 候选隐私预算相加的第二总和, 并基于第一总和和第二总和, 确定该 ε 候选隐私预算是否可用。例如, 若第一总和小于第一预设阈值, 并且第二总和小于第二预设阈值, 则可以确定该 ε 候选隐私预算以及 δ 候选隐私预算可用。若第一总和大于等于第一预设阈值, 或者第二总和大于等于第二预设阈值, 则可以确定该 ε 候选隐私预算以及 δ 候选隐私预算不可用。

[75] 最后, 若 ε 候选隐私预算以及 δ 候选隐私预算可用, 可以将该 ε 候选隐私预算作为第 $n+1$ 轮的 ε 隐私预算, 将该 δ 候选隐私预算作为第 $n+1$ 轮的 δ 隐私预算。例如, 如果第 n 轮的隐私预算为 ε_n 和 δ_n , 候选隐私预算为 $\varepsilon_n + \Delta_\varepsilon$ 和 $\delta_n + \Delta_\delta$, 则可以将 $\varepsilon + \Delta_\varepsilon$ 和 $\delta + \Delta_\delta$ 作为第 $n+1$ 轮的隐私预算, 即:

$$\varepsilon_{n+1} = \varepsilon_n + \Delta_\varepsilon,$$

$$\delta_{n+1} = \delta_n + \Delta_\delta.$$

[76] 在又一种实现方式中, 如果采用 (ε, δ) -本地差分隐私的方法对隐私数据进行差分隐私处理, 该向用户设备发送的隐私预算包括 ε 本地隐私预算以及 δ 隐私预算, 该候选隐私预算包括 ε 候选全局隐私预算以及 δ 候选隐私预算。其中, 该 ε 本地隐私预算可以由 ε 全局隐私预算转换得到, 并且, ε 本地隐私预算和 ε 全局隐私预算正相关。因此, 可以按照增大第 n 轮的 ε 全局隐私预算的方向 (即增大第 n 轮的 ε 本地隐私预算的方向) 确定 ε 候选全局隐私预算。以及按照增大第 n 轮的 δ 隐私预算的方向确定 δ 候选隐私预算。例如, 第 n 轮的隐私预算为 ε_n 和 δ_n , 其中, ε_n 为 ε 本地隐私预算, 设 ε_n' 为第 n 轮的 ε 全局隐私预算, 满足 $\varepsilon_n' = f(\varepsilon_n)$ 。候选隐私预算可以包括 ε 候选全局隐私预算以及 δ 候选隐私预算, 那么, 候选隐私预算可以确定为 $f(\varepsilon_n) + \Delta_\varepsilon$ 和 $\delta + \Delta_\delta$, 其中, $\Delta_\varepsilon > 0$, $\Delta_\delta > 0$ 。

[77] 然后, 一方面, 可以确定该分析阶段已执行完成的各轮操作的 ε 全局隐私预算的总和, 并确定该 ε 全局隐私预算的总和与该 ε 候选全局隐私预算相加得到的第一求和结果。另一方面, 可以确定该分析阶段已执行完成的各轮操作的 δ 隐私预算的总和, 并确定该 δ 隐私预算的总和与该 δ 候选隐私预算相加得到的第二求和结果。再根据第一求和结果和第二求和结果, 确定该 ε 全局候选隐私预算和该 δ 候选隐私预算是否可用。例如, 若第一求和结果小于第一预设阈值, 并且第二求和结果小于第二预设阈值, 则可以确定该 ε 候选全局隐私预算以及 δ 候选隐私预算可用。若第一求和结果大于等于第一预设阈值, 或者第二求和结果大于等于第二预设阈值, 则可以确定该 ε 候选全局隐私预算以及 δ 候选隐私预算不可用。

[78] 最后, 一方面, 可以基于 ε 候选全局隐私预算以及 δ 候选隐私预算, 确定用于用户设备的第 $n+1$ 轮的 ε 本地隐私预算。另一方面, 可以将 δ 候选隐私预算作为第 $n+1$ 轮的 δ 隐私预算。

[79] 需要说明的是, 对于与图 2 实施例相同的步骤, 在上述图 3 实施例中不再进行赘述, 相关内容可参见图 2 实施例。

[80] 本说明书的上述实施例提供的基于差分隐私的业务分析方法, 通过获取目标数据, 对目标数据进行预设的业务分析。若该业务分析成功, 结束该业务分析阶段。若该业务分析失败, 按照增大第 n 轮的隐私预算的方向确定候选隐私预算, 并判断该候选隐私预算是否可用。若该候选隐私预算可用, 基于该候选隐私预算确定第 $n+1$ 轮的隐私预算, 并向该多个用户设备发送第 $n+1$ 轮的隐私预算。从而能够在对数据进行差分隐私处理的过程中, 在保证隐私保护水平较高的前提下, 自适应地调整隐私预算, 进一步增强了隐私保护过程的灵活性, 有助于提高隐私保护数据的可用性。

[81] 如图 4 所示, 图 4 根据一示例性实施例示出的另一种基于差分隐私的业务分析方法

的流程图，该实施例详细描述 ϵ 、 δ -本地差分隐私处理的过程，该方法可以应用于云端平台中，包括以下步骤：在步骤401中，获取目标数据。

[82]在本实施例中，目标数据为对待处理数据进行匿名化处理而得到的。其中，待处理数据可以包括多个用户设备各自上传的各组差分隐私数据，任一组差分隐私数据由对应的用户设备利用第 n 轮的 ϵ 本地隐私预算以及 δ 隐私预算，对该业务分析阶段中该用户设备的隐私数据进行本地差分隐私处理得到。

[83]在步骤402中，对目标数据进行预设的业务分析。

[84]在本实施例中，可以对目标数据进行预设的业务分析。具体来说，可以对目标数据进行统计计算分析，和/或对目标数据进行分类预测。

[85]在步骤403中，若该业务分析成功，结束该业务分析阶段。

[86]在步骤404中，若该业务分析失败，确定 ϵ 候选全局隐私预算以及 δ 候选隐私预算。

[87]在本实施例中，若该业务分析失败，可以确定 ϵ 候选全局隐私预算以及 δ 候选隐私预算，使 ϵ 候选全局隐私预算大于当前存储的第 n 轮 ϵ 全局隐私预算，使 δ 候选隐私预算大于第 n 轮 δ 隐私预算。

[88]在步骤405中，判断 ϵ 候选全局隐私预算和 δ 候选隐私预算是否可用。

[89]在一种实现方式中，可以确定该分析阶段已执行完成的各轮操作的 ϵ 全局隐私预算的总和，并确定该 ϵ 全局隐私预算的总和与该 ϵ 候选全局隐私预算相加得到的第一求和结果。以及，确定该分析阶段已执行完成的各轮操作的 δ 隐私预算的总和，并确定该 δ 隐私预算的总和与该 δ 候选隐私预算相加得到的第二求和结果。然后，根据第一求和结果和第二求和结果，确定该 ϵ 候选全局隐私预算和该 δ 候选隐私预算是否可用。例如，若第一求和结果小于第一预设阈值，并且第二求和结果小于第二预设阈值，则可以确定该 ϵ 候选全局隐私预算以及 δ 候选隐私预算可用。若第一求和结果大于等于第一预设阈值，或者第二求和结果大于等于第二预设阈值，则可以确定该 ϵ 候选全局隐私预算以及 δ 候选隐私预算不可用。

[90]在另一种实现方式中，还可以确定该分析阶段已执行完成的各轮操作的 ϵ 全局隐私预算及 ϵ 候选全局隐私预算的加权和，将该加权和与预设矫正项相加的结果作为第一结果。其中，该预设矫正项与该分析阶段已执行完成的各轮操作的 ϵ 全局隐私预算及 ϵ 候选全局隐私预算的平方和正相关。确定该分析阶段已执行完成的各轮操作的 δ 隐私预算及 δ 候选隐私预算的总和，作为第二结果。若第一结果小于第一预设值，并且第二结果小于第二预设值，则确定 ϵ 候选全局隐私预算以及 δ 候选隐私预算可用。若第一结果大于等于第一预设值，或者第二结果大于等于第二预设值，则确定 ϵ 候选全局隐私预算以及 δ 候选隐私预算不可用。

[91]可以理解，还可以通过其它任意合理的方式判断 ϵ 候选全局隐私预算以及 δ 候选隐私预算是否可用，本实施例对判断 ϵ 候选全局隐私预算以及 δ 候选隐私预算是否可用的具体方式方面不限定。

[92]在步骤406中，若 ϵ 候选全局隐私预算以及 δ 候选隐私预算可用，基于 ϵ 候选全局隐私预算以及 δ 候选隐私预算，确定用于用户设备的第 $n+1$ 轮的 ϵ 本地隐私预算，并将 ϵ 候选全局隐私预算存储为第 $n+1$ 轮 ϵ 全局隐私预算，将 δ 候选隐私预算作为第 $n+1$ 轮的 δ 隐私预算。

[93]在本实施例中，若 ϵ 候选全局隐私预算以及 δ 候选隐私预算可用，可以将 δ 候选隐私预算作为第 $n+1$ 轮的 δ 隐私预算。并可以基于该 ϵ 候选全局隐私预算以及 δ 候选隐私预算，确定用于用户设备的第 $n+1$ 轮的 ϵ 本地隐私预算。具体来说，可以基于 δ 候选隐

私预算, 确定目标系数。该目标系数与 δ 候选隐私预算正相关, 与多个用户设备的数目正相关。然后, 将 ϵ 候选全局隐私预算与目标系数相乘, 得到用于用户设备的第 $n+1$ 轮的 ϵ 本地隐私预算。

[94] 例如, 可以通过如下公式确定用于用户设备的第 $n+1$ 轮的 ϵ 本地隐私预算:

$$\epsilon_1 = \frac{\epsilon_2}{12\sqrt{\frac{1}{\ln \frac{\Delta}{m}}}}$$

[95] 其中, ϵ_1 表示第 $n+1$ 轮的 ϵ 本地隐私预算, ϵ_2 表示 ϵ 候选全局隐私预算, Δ 表示 δ 候选隐私预算, m 表示用户设备的数目。可以理解, 确定用于用户设备的第 $n+1$ 轮的 ϵ 本地隐私预算的具体方式并不限于上述公式, 其它任意对上述公式进行的合理的变形, (例如, 上述公式中的 12 也可以是根据经验确定的其它数值, 上述公式中的 m 也可以是与用户设备的数目相同量级的一个常数, 等等) 均可以适用于本实施例, 本实施例对确定第 $n+1$ 轮的 ϵ 本地隐私预算的具体方式方面不限定。

[96] 在本实施例中, 可以将 ϵ 候选全局隐私预算存储为第 $n+1$ 轮 ϵ 全局隐私预算, 以便于确定第 $n+1$ 轮的候选隐私预算。

[97] 需要说明的是, 对于与图 2 和图 3 实施例中相同的步骤, 在上述图 4 实施例中不再进行赘述, 相关内容可参见图 2 和图 3 实施例。

[98] 本说明书的上述实施例提供的基于差分隐私的业务分析方法, 通过获取目标数据, 对目标数据进行预设的业务分析。若该业务分析成功, 结束该业务分析阶段, 若该业务分析失败, 确定 ϵ 候选全局隐私预算以及 δ 候选隐私预算。判断 ϵ 候选全局隐私预算和 δ 候选隐私预算是否可用, 若 ϵ 候选全局隐私预算以及 δ 候选隐私预算可用, 基于 ϵ 候选全局隐私预算以及 δ 候选隐私预算, 确定用于用户设备的第 $n+1$ 轮的 ϵ 本地隐私预算, 并将 ϵ 候选全局隐私预算存储为第 $n+1$ 轮 ϵ 全局隐私预算, 将 δ 候选隐私预算作为第 $n+1$ 轮的 δ 隐私预算。从而能够在对数据进行差分隐私处理的过程中, 自适应地调整隐私预算, 进一步增强了隐私保护过程的灵活性, 有助于提高隐私保护数据的可用性。

[99] 应当注意, 尽管在上述实施例中, 以特定顺序描述了本说明书实施例的方法的操作, 但是, 这并非要求或者暗示必须按照该特定顺序来执行这些操作, 或是必须执行全部所示的操作才能实现期望的结果。相反, 流程图中描绘的步骤可以改变执行顺序。附加地或备选地, 可以省略某些步骤, 将多个步骤合并为一个步骤执行, 和/或将一个步骤分解为多个步骤执行。

[100] 与前述基于差分隐私的业务分析方法实施例相对应, 本说明书还提供了基于差分隐私的业务分析装置的实施例。

[101] 如图 5 所示, 图 5 是本说明书根据一示例性实施例示出的一种基于差分隐私的业务分析装置框图, 该装置执行至少一个业务分析阶段, 任一个业务分析阶段包括至少一轮操作。针对该业务分析阶段的第 n 轮的操作, 其中, n 大于等于 1, 该装置可以包括: 获取模块 501, 分析模块 502, 结束模块 503, 确定模块 504 和发送模块 505。

[102] 其中, 获取模块 501, 用于获取目标数据, 目标数据为对待处理数据进行匿名化处理得到的。该待处理数据包括多个用户设备各自上传的各组差分隐私数据。任一组差分隐私数据由对应的用户设备利用第 n 轮的隐私预算, 对该业务分析阶段中该用户设备的隐私数据进行差分隐私处理得到。

[103] 分析模块 502, 用于对目标数据进行预设的业务分析。

- [104] 结束模块 503, 用于在业务分析成功时, 结束该业务分析阶段。
- [105] 确定模块 504, 用于在业务分析失败时, 确定第 $n+1$ 轮的隐私预算。
- [106] 发送模块 505, 用于向多个用户设备发送第 $n+1$ 轮的隐私预算, 使各个用户设备重新对该业务分析阶段中各自的隐私数据进行差分隐私处理, 以进行第 $n+1$ 轮的操作。
- [107] 在一些实施方式中, 确定模块 504 可以包括: 第一确定子模块, 判断子模块和第二确定子模块 (图中未示出)。
- [108] 其中, 第一确定子模块, 用于按照增大第 n 轮的隐私预算的方向确定候选隐私预算。
- [109] 判断子模块, 用于判断候选隐私预算是否可用。
- [110] 第二确定子模块, 用于在候选隐私预算可用时, 基于候选隐私预算确定第 $n+1$ 轮的隐私预算。
- [111] 在另一些实施方式中, 判断子模块被配置用于: 确定该分析阶段已执行完成的各轮操作的隐私预算的总和, 并基于该总和与候选隐私预算相加得到的结果, 确定候选隐私预算是否可用。
- [112] 在另一些实施方式中, 上述差分隐私处理为 ϵ, δ -本地差分隐私处理, 上述隐私预算包括 ϵ 本地隐私预算以及 δ 隐私预算, 上述候选隐私预算包括 ϵ 候选全局隐私预算以及 δ 候选隐私预算。
- [113] 其中, 第一确定子模块被配置用于: 确定 ϵ 候选全局隐私预算以及 δ 候选隐私预算, 使 ϵ 候选全局隐私预算大于当前存储的第 n 轮 ϵ 全局隐私预算, 使 δ 候选隐私预算大于第 n 轮 δ 隐私预算。
- [114] 其中, 判断子模块被配置用于: 判断 ϵ 候选全局隐私预算以及 δ 候选隐私预算是否可用。
- [115] 其中, 第二确定子模块被配置用于: 若 ϵ 候选全局隐私预算以及 δ 候选隐私预算可用, 基于 ϵ 候选全局隐私预算以及 δ 候选隐私预算, 确定用于上述用户设备的第 $n+1$ 轮的 ϵ 本地隐私预算, 并将 ϵ 候选全局隐私预算存储为第 $n+1$ 轮的 ϵ 全局隐私预算, 将 δ 候选隐私预算作为第 $n+1$ 轮的 δ 隐私预算。
- [116] 在另一些实施方式中, 判断子模块可以通过如下方式判断 ϵ 候选全局隐私预算以及 δ 候选隐私预算是否可用: 确定该分析阶段已执行完成的各轮操作的 ϵ 全局隐私预算及 ϵ 候选全局隐私预算的加权和, 将上述加权和与预设矫正项相加的结果作为第一结果。其中, 该预设矫正项与该分析阶段已执行完成的各轮操作的 ϵ 全局隐私预算及 ϵ 候选全局隐私预算的平方和正相关。确定该分析阶段已执行完成的各轮操作的 δ 隐私预算及 δ 候选隐私预算的总和, 作为第二结果。若第一结果小于第一预设值, 并且第二结果小于第二预设值, 则确定 ϵ 候选全局隐私预算以及 δ 候选隐私预算可用。
- [117] 在另一些实施方式中, 第二确定子模块可以通过如下方式基于 ϵ 候选全局隐私预算以及 δ 候选隐私预算, 确定用于用户设备的第 $n+1$ 轮的 ϵ 本地隐私预算: 基于 δ 候选隐私预算, 确定目标系数, 该目标系数与 δ 候选隐私预算正相关, 目标系数与多个用户设备的数目正相关。将 ϵ 候选全局隐私预算与目标系数相乘, 得到第 $n+1$ 轮的 ϵ 本地隐私预算。
- [118] 在另一些实施方式中, 获取模块 501 被配置用于: 在可信执行环境中获取待处理数据, 并在该可信执行环境中对该待处理数据进行匿名化处理, 得到目标数据。
- [119] 在另一些实施方式中, 分析模块 502 被配置用于: 对目标数据进行统计计算分析;

和/或对目标数据进行分类预测。

[120] 在另一些实施方式中，任一个用户设备的隐私数据可以包括以下一项或多项：通过该用户设备输入的文本数据；通过该用户设备输入的表情符号；通过该用户设备点击链接的信息；在该用户设备上运行应用程序的信息；利用该用户设备收付款的信息；通过该用户设备浏览网页的信息；通过该用户设备搜索的信息；利用该用户设备播放音视频的信息；该用户设备的定位数据；利用该用户设备购买商品的信息。

[121] 应当理解，上述装置可以预先设置在云端平台的计算设备中，也可以通过下载等方式而加载到云端平台的计算设备中。上述装置中的相应模块可以与云端平台的计算设备中的模块相互配合以实现基于差分隐私的业务分析方案。

[122] 对于装置实施例而言，由于其基本对应于方法实施例，所以相关之处参见方法实施例的部分说明即可。以上所描述的装置实施例仅仅是示意性的，其中所述作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部模块来实现本说明书一个或多个实施例方案的目的。本领域普通技术人员在不付出创造性劳动的情况下，即可以理解并实施。

[123] 本说明书一个或多个实施例还提供了一种计算机可读存储介质，该存储介质存储有计算机程序，计算机程序可用于执行上述图 2 至图 4 任一实施例提供的基于差分隐私的业务分析方法。

[124] 对应于上述的基于差分隐私的业务分析方法，本说明书一个或多个实施例还提出了图 6 所示的根据本说明书的一示例性实施例的计算设备的示意结构图。请参考图 6，在硬件层面，该计算设备包括处理器、内部总线、网络接口、内存以及非易失性存储器，当然还可能包括其他业务所需要的硬件。处理器从非易失性存储器中读取对应的计算机程序到内存中然后运行，在逻辑层面上形成基于差分隐私的业务分析装置。当然，除了软件实现方式之外，本说明书一个或多个实施例并不排除其他实现方式，比如逻辑器件抑或软硬件结合的方式等等，也就是说以下处理流程的执行主体并不限定于各个逻辑单元，也可以是硬件或逻辑器件。

[125] 本说明书中的各个实施例均采用递进的方式描述，各个实施例之间相同相似的部分互相参见即可，每个实施例重点说明的都是与其他实施例的不同之处。尤其，对于系统实施例而言，由于其基本相似于方法实施例，所以描述的比较简单，相关之处参见方法实施例的部分说明即可。

[126] 上述对本说明书特定实施例进行了描述。其它实施例在所附权利要求书的范围内。在一些情况下，在权利要求书中记载的动作或步骤可以按照不同于实施例中的顺序来执行并且仍然可以实现期望的结果。另外，在附图中描绘的过程不一定要求示出的特定顺序或者连续顺序才能实现期望的结果。在某些实施方式中，多任务处理和并行处理也是可以的或者可能是有利的。

[127] 本领域普通技术人员应该还可以进一步意识到，结合本文中所公开的实施例描述的各示例的单元及算法步骤，能够以电子硬件、计算机软件或者二者的结合来实现，为了清楚地说明硬件和软件的可互换性，在上述说明中已经按照功能一般性地描述了各示例的组成及步骤。这些功能究竟以硬件还是软件方式来执行，取决于技术方案的特定应用和设计约束条件。本领域普通技术人员可以对每个特定的应用来使用不同方法来实现所描述的功能，但是这种实现不应认为超出本申请的范围。其中，软件模块可以置于随机存储器（RAM）、内存、只读存储器（ROM）、电可编程 ROM、电可擦除可编程 ROM、寄存器、硬盘、可移动磁盘、CD-ROM、或技术领域内所公知的任意其它形式的

存储介质中。

[128] 以上所述的具体实施方式，对本申请的目的、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，以上所述仅为本申请的具体实施方式而已，并不用于限定本申请的保护范围，凡在本申请的精神和原则之内，所做的任何修改、等同替换、改进等，均应包含在本申请的保护范围之内。

权利要求书

1. 一种基于差分隐私的业务分析方法，所述方法包括至少一个业务分析阶段，任一个业务分析阶段包括至少一轮操作；该业务分析阶段的第 n 轮的操作包括以下步骤，其中， n 大于等于 1：

获取目标数据；所述目标数据为对待处理数据进行匿名化处理得到的；所述待处理数据包括多个用户设备各自上传的各组差分隐私数据；任一组差分隐私数据由对应的用户设备利用第 n 轮的隐私预算，对该业务分析阶段中该用户设备的隐私数据进行差分隐私处理得到；

对所述目标数据进行预设的业务分析；

若所述业务分析成功，结束该业务分析阶段；

若所述业务分析失败，确定第 $n+1$ 轮的隐私预算，并向所述多个用户设备发送所述第 $n+1$ 轮的隐私预算，使各个用户设备重新对该业务分析阶段中各自的隐私数据进行差分隐私处理，以进行第 $n+1$ 轮的操作。

2. 根据权利要求 1 所述的方法，其中，所述确定第 $n+1$ 轮的隐私预算，包括：

按照增大所述第 n 轮的隐私预算的方向确定候选隐私预算；

判断所述候选隐私预算是否可用；

若所述候选隐私预算可用，基于所述候选隐私预算确定所述第 $n+1$ 轮的隐私预算。

3. 根据权利要求 2 所述的方法，其中，所述判断所述候选隐私预算是否可用，包括：

确定该分析阶段已执行完成的各轮操作的隐私预算的总和；

基于所述总和与所述候选隐私预算相加得到的结果，确定所述候选隐私预算是否可用。

4. 根据权利要求 2 所述的方法，其中，所述差分隐私处理为 ϵ, δ -本地差分隐私处理；所述隐私预算包括 ϵ 本地隐私预算以及 δ 隐私预算；所述候选隐私预算包括 ϵ 候选全局隐私预算以及 δ 候选隐私预算；

其中，所述确定候选隐私预算，包括：

确定 ϵ 候选全局隐私预算以及 δ 候选隐私预算，使所述 ϵ 候选全局隐私预算大于当前存储的第 n 轮 ϵ 全局隐私预算，使所述 δ 候选隐私预算大于第 n 轮 δ 隐私预算；

其中，所述判断所述候选隐私预算是否可用，包括：

判断所述 ϵ 候选全局隐私预算以及所述 δ 候选隐私预算是否可用；

其中，所述若所述候选隐私预算可用，基于所述候选隐私预算确定所述第 $n+1$ 轮的隐私预算，包括：

若所述 ϵ 候选全局隐私预算以及所述 δ 候选隐私预算可用，基于所述 ϵ 候选全局隐私预算以及所述 δ 候选隐私预算，确定用于所述用户设备的第 $n+1$ 轮的 ϵ 本地隐私预算，并将所述 ϵ 候选全局隐私预算存储为第 $n+1$ 轮的 ϵ 全局隐私预算；将 δ 候选隐私预算作为第 $n+1$ 轮的 δ 隐私预算。

5. 根据权利要求 4 所述的方法，其中，所述判断所述 ϵ 候选全局隐私预算以及所述 δ 候选隐私预算是否可用，包括：

确定该分析阶段已执行完成的各轮操作的 ϵ 全局隐私预算及所述 ϵ 候选全局隐私预算的加权和，将所述加权和与预设矫正项相加的结果作为第一结果；其中，所述预设矫正项与该分析阶段已执行完成的各轮操作的 ϵ 全局隐私预算及所述 ϵ 候选全局隐私预算的平方和正相关；

确定该分析阶段已执行完成的各轮操作的 δ 隐私预算及所述 δ 候选隐私预算的总和，作为第二结果；

若所述第一结果小于第一预设值，并且所述第二结果小于第二预设值，则确定所述 ϵ 候选全局隐私预算以及所述 δ 候选隐私预算可用。

6. 根据权利要求4所述的方法, 其中, 所述基于所述 ϵ 候选全局隐私预算以及所述 δ 候选隐私预算, 确定用于所述用户设备的第 $n+1$ 轮的 ϵ 本地隐私预算, 包括:

基于所述 δ 候选隐私预算, 确定目标系数; 所述目标系数与所述 δ 候选隐私预算正相关; 所述目标系数与所述多个用户设备的数目正相关;

将所述 ϵ 候选全局隐私预算与所述目标系数相乘, 得到所述第 $n+1$ 轮的 ϵ 本地隐私预算。

7. 根据权利要求1所述的方法, 其中, 所述获取目标数据, 包括:

在可信执行环境中获取所述待处理数据, 并在所述可信执行环境中对所述待处理数据进行匿名化处理, 得到所述目标数据。

8. 根据权利要求1中任一项所述的方法, 其中, 对所述目标数据进行预设的业务分析, 包括:

对所述目标数据进行统计计算分析; 和/或

对所述目标数据进行分类预测。

9. 根据权利要求1至8中任一项所述的方法, 其中, 任一个用户设备的隐私数据包括以下一项或多项:

通过该用户设备输入的文本数据;

通过该用户设备输入的表情符号;

通过该用户设备点击链接的信息;

在该用户设备上运行应用程序的信息;

利用该用户设备收付款的信息;

通过该用户设备浏览网页的信息;

通过该用户设备搜索的信息;

利用该用户设备播放音视频的信息;

该用户设备的定位数据;

利用该用户设备购买商品的信息。

10. 一种基于差分隐私的业务分析装置, 所述装置执行至少一个业务分析阶段, 任一个业务分析阶段包括至少一轮操作; 针对该业务分析阶段的第 n 轮的操作, 其中, n 大于等于1, 所述装置包括:

获取模块, 用于获取目标数据; 所述目标数据为对待处理数据进行匿名化处理得到的; 所述待处理数据包括多个用户设备各自上传的各组差分隐私数据; 任一组差分隐私数据由对应的用户设备利用第 n 轮的隐私预算, 对该业务分析阶段中该用户设备的隐私数据进行差分隐私处理得到;

分析模块, 用于对所述目标数据进行预设的业务分析;

结束模块, 用于在所述业务分析成功时, 结束该业务分析阶段;

确定模块, 用于在所述业务分析失败时, 确定第 $n+1$ 轮的隐私预算;

发送模块, 用于向所述多个用户设备发送所述第 $n+1$ 轮的隐私预算, 使各个用户设备重新对该业务分析阶段中各自的隐私数据进行差分隐私处理, 以进行第 $n+1$ 轮的操作。

11. 根据权利要求10所述的装置, 其中, 所述确定模块包括:

第一确定子模块, 用于按照增大所述第 n 轮的隐私预算的方向确定候选隐私预算;

判断子模块, 用于判断所述候选隐私预算是否可用;

第二确定子模块, 用于在所述候选隐私预算可用时, 基于所述候选隐私预算确定所述第 $n+1$ 轮的隐私预算。

12. 根据权利要求11所述的装置, 其中, 所述判断子模块被配置用于:

确定该分析阶段已执行完成的各轮操作的隐私预算的总和;

基于所述总和与所述候选隐私预算相加得到的结果, 确定所述候选隐私预算是否可

用。

13. 根据权利要求 11 所述的装置, 其中, 所述差分隐私处理为 ϵ, δ -本地差分隐私处理; 所述隐私预算包括 ϵ 本地隐私预算以及 δ 隐私预算; 所述候选隐私预算包括 ϵ 候选全局隐私预算以及 δ 候选隐私预算;

其中, 所述第一确定子模块被配置用于:

确定 ϵ 候选全局隐私预算以及 δ 候选隐私预算, 使所述 ϵ 候选全局隐私预算大于当前存储的第 n 轮 ϵ 全局隐私预算, 使所述 δ 候选隐私预算大于第 n 轮 δ 隐私预算;

其中, 所述判断子模块被配置用于:

判断所述 ϵ 候选全局隐私预算以及所述 δ 候选隐私预算是否可用;

其中, 所述第二确定子模块被配置用于:

若所述 ϵ 候选全局隐私预算以及所述 δ 候选隐私预算可用, 基于所述 ϵ 候选全局隐私预算以及所述 δ 候选隐私预算, 确定用于所述用户设备的第 $n+1$ 轮的 ϵ 本地隐私预算, 并将所述 ϵ 候选全局隐私预算存储为第 $n+1$ 轮的 ϵ 全局隐私预算; 将 δ 候选隐私预算作为第 $n+1$ 轮的 δ 隐私预算。

14. 根据权利要求 13 所述的装置, 其中, 所述判断子模块通过如下方式判断所述 ϵ 候选全局隐私预算以及所述 δ 候选隐私预算是否可用:

确定该分析阶段已执行完成的各轮操作的 ϵ 全局隐私预算及所述 ϵ 候选全局隐私预算的加权和, 将所述加权和与预设矫正项相加的结果作为第一结果; 其中, 所述预设矫正项与该分析阶段已执行完成的各轮操作的 ϵ 全局隐私预算及所述 ϵ 候选全局隐私预算的平方和正相关;

确定该分析阶段已执行完成的各轮操作的 δ 隐私预算及所述 δ 候选隐私预算的总和, 作为第二结果;

若所述第一结果小于第一预设值, 并且所述第二结果小于第二预设值, 则确定所述 ϵ 候选全局隐私预算以及所述 δ 候选隐私预算可用。

15. 根据权利要求 13 所述的装置, 其中, 所述第二确定子模块通过如下方式基于所述 ϵ 候选全局隐私预算以及所述 δ 候选隐私预算, 确定用于所述用户设备的第 $n+1$ 轮的 ϵ 本地隐私预算:

基于所述 δ 候选隐私预算, 确定目标系数; 所述目标系数与所述 δ 候选隐私预算正相关; 所述目标系数与所述多个用户设备的数目正相关;

将所述 ϵ 候选全局隐私预算与所述目标系数相乘, 得到所述第 $n+1$ 轮的 ϵ 本地隐私预算。

16. 根据权利要求 10 所述的装置, 其中, 所述获取模块被配置用于:

在可信执行环境中获取所述待处理数据, 并在所述可信执行环境中对所述待处理数据进行匿名化处理, 得到所述目标数据。

17. 根据权利要求 10 中任一项所述的装置, 其中, 所述分析模块被配置用于:

对所述目标数据进行统计计算分析; 和/或

对所述目标数据进行分类预测。

18. 根据权利要求 10 至 17 中任一项所述的装置, 其中, 任一个用户设备的隐私数据包括以下一项或多项:

通过该用户设备输入的文本数据;

通过该用户设备输入的表情符号;

通过该用户设备点击链接的信息;

在该用户设备上运行应用程序的信息;

利用该用户设备收付款的信息;

通过该用户设备浏览网页的信息;

通过该用户设备搜索的信息;

利用该用户设备播放音视频的信息；

该用户设备的定位数据；

利用该用户设备购买商品的信息。

19. 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，令所述计算机执行权利要求 1 至 9 中任一项所述的方法。

20. 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，实现权利要求 1 至 9 中任一项所述的方法。