(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 115664743 A
(43)申请公布日 2023.01.31

(21)申请号 202211268787.0

(22)申请日 2022.10.17

(71)申请人 浙江网商银行股份有限公司
地址 310012 浙江省杭州市西湖区古荡街道西溪路556号阿里中心D幢9层、E幢3-8层

(72)发明人 陈怡航 张园超

(74)专利代理机构 北京智信禾专利代理有限公司 11637
专利代理师 张瑞

(51)Int.Cl.
H04L 9/40(2022.01)

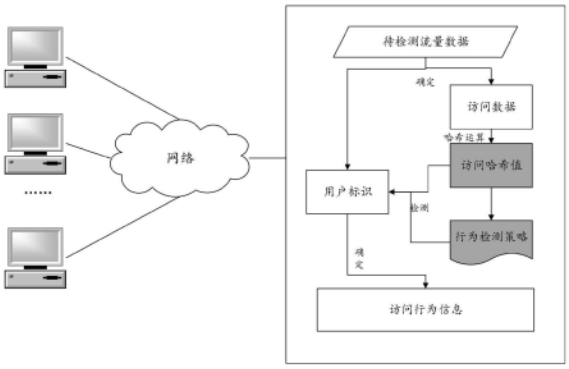
权利要求书3页 说明书15页 附图3页

(54)发明名称

行为检测方法以及装置

(57)摘要

本说明书实施例提供行为检测方法以及装置，其中所述行为检测方法包括：获取目标业务对应的待检测流量数据；在所述待检测流量数据中确定用户标识，以及所述用户标识关联的访问数据；对所述访问数据进行哈希运算，获得所述用户标识对应的访问哈希值；基于所述目标业务的行为检测策略和所述访问哈希值，确定所述用户标识的访问行为信息；其中，所述行为检测策略关联水平越权行为检测维度。



CN 115664743 A

1.一种行为检测方法,包括:

获取目标业务对应的待检测流量数据;

在所述待检测流量数据中确定用户标识,以及所述用户标识关联的访问数据;

对所述访问数据进行哈希运算,获得所述用户标识对应的访问哈希值;

基于所述目标业务的行为检测策略和所述访问哈希值,确定所述用户标识的访问行为信息;其中,所述行为检测策略关联水平越权行为检测维度。

2.根据权利要求1所述的方法,所述获取目标业务对应的待检测流量数据步骤执行之前,还包括:

获取所述目标业务的历史流量数据;

在所述历史流量数据中确定关联用户资源的资源访问数据,并基于所述资源访问数据生成基准访问信息;

相应的,所述获取目标业务对应的待检测流量数据,包括:

获取所述目标业务对应的初始流量数据;

在所述初始流量数据中筛选出关联所述基准访问信息的流量数据,作为所述待检测流量数据。

3.根据权利要求1所述的方法,所述在所述待检测流量数据中确定用户标识,以及所述用户标识关联的访问数据,包括:

在所述待检测流量数据对应的用户信息文件中提取会话标识,并确定所述会话标识对应的所述用户标识;

对所述待检测流量数据进行解析,根据解析结果生成所述用户标识关联的所述访问数据。

4.根据权利要求3所述的方法,所述对所述待检测流量数据进行解析,根据解析结果生成所述用户标识关联的所述访问数据,包括:

对所述待检测流量数据进行解析,获得所述用户标识关联的访问地址、访问参数信息以及访问参数值;

通过对所述访问地址、所述访问参数信息和所述访问参数值进行拼接,获得所述用户标识关联的所述访问数据。

5.根据权利要求1所述的方法,在所述目标业务所属的业务方满足资源调用条件的情况下,所述基于所述目标业务的行为检测策略和所述访问哈希值,确定所述用户标识的访问行为信息,包括:

基于所述目标业务的行为检测策略确定访问信息表;

根据所述访问哈希值查询所述访问信息表,根据查询结果确定所述用户标识的访问行为信息;

其中,所述访问信息表记录历史访问哈希值和历史用户标识之间的映射关系。

6.根据权利要求5所述的方法,所述根据查询结果确定所述用户标识的访问行为信息,包括:

根据查询结果确定关联用户标识,在所述关联用户标识与所述用户标识相同的情况下,确定访问正常信息作为所述用户标识的访问行为信息;或者,

根据查询结果确定关联用户标识,在所述关联用户标识与所述用户标识不相同的情况

下,确定访问异常信息作为所述用户标识的访问行为信息;或者,

根据查询结果确定所述访问信息表中不存在关联用户标识的情况下,基于所述用户标识和所述访问哈希值生成目标映射关系,并将所述目标映射关系记录至所述访问信息表。

7.根据权利要求1所述的方法,在所述目标业务所属的业务方不满足资源调用条件的情况下,所述基于所述目标业务的行为检测策略和所述访问哈希值,确定所述用户标识的访问行为信息,包括:

根据所述待检测流量数据,确定预设时间区间内所述访问哈希值对应的用户标识数量;

基于所述行为检测策略对所述用户标识数量进行检测,根据检测结果确定所述用户标识的访问行为信息。

8.根据权利要求7所述的方法,所述根据所述待检测流量数据,确定预设时间区间内所述访问哈希值对应的用户标识数量,包括:

根据所述待检测流量数据,确定预设时间区间内所述访问数据对应的访问用户标识;

统计所述访问用户标识对应的标识数量,作为所述访问哈希值对应的用户标识数量。

9.根据权利要求8所述的方法,所述基于所述行为检测策略对所述用户标识数量进行检测,根据检测结果确定所述用户标识的访问行为信息,包括:

基于所述行为检测策略确定所述用户标识数量大于预设数量阈值的情况下,确定访问异常信息作为所述用户标识的访问行为信息;或者,

基于所述行为检测策略确定所述用户标识数量小于等于预设数量阈值的情况下,确定访问正常信息作为所述用户标识的访问行为信息。

10.根据权利要求9所述的方法,所述确定访问异常信息作为所述用户标识的访问行为信息步骤执行之后,还包括:

获取所述访问数据对应每个访问用户标识的访问反馈结果;

对每个访问用户标识的访问反馈结果分别进行哈希运算,获得每个访问用户标识对应的反馈哈希值;

将每个访问用户标识对应的反馈哈希值进行比较,根据比较结果确定所述用户标识的异常行为结果。

11.一种行为检测装置,包括:

获取数据模块,被配置为获取目标业务对应的待检测流量数据;

确定标识模块,被配置为在所述待检测流量数据中确定用户标识,以及所述用户标识关联的访问数据;

哈希运算模块,被配置为对所述访问数据进行哈希运算,获得所述用户标识对应的访问哈希值;

确定信息模块,被配置为基于所述目标业务的行为检测策略和所述访问哈希值,确定所述用户标识的访问行为信息;其中,所述行为检测策略关联水平越权行为检测维度。

12.一种计算设备,包括:

存储器和处理器;

所述存储器用于存储计算机可执行指令,所述处理器用于执行所述计算机可执行指令,该计算机可执行指令被处理器执行时实现权利要求1至10任意一项所述方法的步骤。

13.一种计算机可读存储介质,其存储有计算机可执行指令,该计算机可执行指令被处理器执行时实现权利要求1至10任意一项所述方法的步骤。

行为检测方法以及装置

技术领域

[0001] 本说明书实施例涉及计算机技术领域，特别涉及行为检测方法以及装置。

背景技术

[0002] 随着互联网技术的发展，越来越多的业务开始线上化，以通过线上业务为用户带来更便捷的服务。而随着线上业务的发展，水平越权漏洞成为了互联网站点普遍存在的问题，不仅会造成线上业务无法正常开展，还会导致用户敏感数据大批量泄露，很大程度会影响线上业务的正常运行。现有技术中，针对水平越权漏洞问题，大多数采用越权行为发生后的维护措施，即水平越权行为发生后，会利用站内预设的修复措施进行处理，以避免造成更多数据的泄露；但是这种处理方式存在一定的滞后性，无法及时止损，因此亟需一种有效的方案以解决上述问题。

发明内容

[0003] 有鉴于此，本说明书实施例提供了一种行为检测方法。本说明书一个或者多个实施例同时涉及一种行为检测装置，一种计算设备，一种计算机可读存储介质以及一种计算机程序，以解决现有技术中存在的技术缺陷。

[0004] 根据本说明书实施例的第一方面，提供了一种行为检测方法，包括：

[0005] 获取目标业务对应的待检测流量数据；

[0006] 在所述待检测流量数据中确定用户标识，以及所述用户标识关联的访问数据；

[0007] 对所述访问数据进行哈希运算，获得所述用户标识对应的访问哈希值；

[0008] 基于所述目标业务的行为检测策略和所述访问哈希值，确定所述用户标识的访问行为信息；其中，所述行为检测策略关联水平越权行为检测维度。

[0009] 根据本说明书实施例的第二方面，提供了一种行为检测装置，包括：

[0010] 获取数据模块，被配置为获取目标业务对应的待检测流量数据；

[0011] 确定标识模块，被配置为在所述待检测流量数据中确定用户标识，以及所述用户标识关联的访问数据；

[0012] 哈希运算模块，被配置为对所述访问数据进行哈希运算，获得所述用户标识对应的访问哈希值；

[0013] 确定信息模块，被配置为基于所述目标业务的行为检测策略和所述访问哈希值，确定所述用户标识的访问行为信息；其中，所述行为检测策略关联水平越权行为检测维度。

[0014] 根据本说明书实施例的第三方面，提供了一种计算设备，包括：

[0015] 存储器和处理器；

[0016] 所述存储器用于存储计算机可执行指令，所述处理器用于执行所述计算机可执行指令时实现任上述行为检测方法的步骤。

[0017] 根据本说明书实施例的第四方面，提供了一种计算机可读存储介质，其存储有计算机可执行指令，该指令被处理器执行时实现上述行为检测方法的步骤。

[0018] 根据本说明书实施例的第五方面，提供了一种计算机程序，其中，当所述计算机程序在计算机中执行时，令计算机执行上述行为检测方法的步骤。

[0019] 本说明书提供的行为检测方法，为了能够提前感知越权行为并作出防护，可以在获取目标业务对应的待检测流量数据后，在待检测流量数据中确定用户标识，以及与用户标识关联的访问数据，之后对访问数据进行哈希运算，得到用户标识对应的访问哈希值，此时实现了针对每条访问数据生成唯一对应关系的哈希值，以方便后续能够进行访问行为检测。此后通过结合目标业务的行为检测策略和访问哈希值，实现在针对访问数据反馈私有资源前，完成对用户标识的访问行为信息的确定，可以达到提前感知越权行为和防护的效果，以避免数据泄露而造成的损失。

附图说明

[0020] 图1是本说明书一个实施例提供的一种行为检测方法的结构示意图；

[0021] 图2是本说明书一个实施例提供的一种行为检测方法的流程图；

[0022] 图3是本说明书一个实施例提供的另一种行为检测方法的流程图；

[0023] 图4是本说明书一个实施例提供的一种行为检测装置的结构示意图；

[0024] 图5是本说明书一个实施例提供的一种计算设备的结构框图。

具体实施方式

[0025] 在下面的描述中阐述了很多具体细节以便于充分理解本说明书。但是本说明书能够以很多不同于在此描述的其它方式来实施，本领域技术人员可以在不违背本说明书内涵的情况下做类似推广，因此本说明书不受下面公开的具体实施的限制。

[0026] 在本说明书一个或多个实施例中使用的术语是仅仅出于描述特定实施例的目的，而非旨在限制本说明书一个或多个实施例。在本说明书一个或多个实施例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，本说明书一个或多个实施例中使用的术语“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。

[0027] 应当理解，尽管在本说明书一个或多个实施例中可能采用术语第一、第二等来描述各种信息，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，在不脱离本说明书一个或多个实施例范围的情况下，第一也可以被称为第二，类似地，第二也可以被称为第一。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”。

[0028] 首先，对本说明书一个或多个实施例涉及的名词术语进行解释。

[0029] Hash(哈希)，是把任意长度的输入(又叫做预映射pre-image)通过散列算法变换成固定长度的输出，该输出就是散列值。这种转换是一种压缩映射，也就是，散列值的空间通常远小于输入的空间，不同的输入可能会散列成相同的输出，所以不可能从散列值来确定唯一的输入值。简单的说就是一种将任意长度的消息压缩到某一固定长度的消息摘要的函数。

[0030] 水平越权：是指同级用户之间的越权，指攻击者尝试访问与他拥有相同权限的用户资源。如，用户A和用户B属于同一级别的角色，拥有相同的权限等级，他们能获取自己的

私有数据(数据A和数据B),但如果系统只验证了能访问数据的角色,而没有对数据做细分或者校验,导致用户A能访问到用户B的数据(数据B),那么用户A访问数据B的这种行为就叫做水平越权访问。

[0031] 在本说明书中,提供了一种行为检测方法,本说明书同时涉及一种行为检测装置,一种计算设备,一种计算机可读存储介质以及一种计算机程序,在下面的实施例中逐一进行详细说明。

[0032] 参见图1所示的示意图,本说明书提供的行为检测方法,为了能够提前感知越权行为并作出防护,可以在获取目标业务对应的待检测流量数据后,在待检测流量数据中确定用户标识,以及与用户标识关联的访问数据,之后对访问数据进行哈希运算,得到用户标识对应的访问哈希值,此时实现了针对每条访问数据生成唯一对应关系的哈希值,以方便后续能够进行访问行为检测。此后通过结合目标业务的行为检测策略和访问哈希值,实现在针对访问数据反馈私有资源前,完成对用户标识的访问行为信息的确定,可以达到提前感知越权行为和防护的效果,以避免数据泄露而造成的损失。

[0033] 图2示出了根据本说明书一个实施例提供的一种行为检测方法的流程图,具体包括以下步骤。

[0034] 步骤S202:获取目标业务对应的待检测流量数据。

[0035] 本说明书提供的行为检测方法应用于网站的行为检测过程,该方法应用于网站所属的服务端,由服务端根据实时采集到的流量数据进行水平越权行为检测,且在检测完成后可以及时熔断,或者对异常行为用户的账号进行封禁等操作,本实施例在此不作任何限定。

[0036] 具体的,目标业务具体是指能够通过使用网站进行资源访问、读取和/或下载等操作的业务,且访问、读取和/或下载等操作涉及到的资源至少包括每个用户所对应的私有资源。即目标业务会涉及到每个用户私有资源的访问、读取和/或下载等操作,该过程可能会发生用户之间的水平越权行为。相应的,待检测流量数据具体是指目标业务在当前时刻所对应的实时流量,用于实现后续可以通过分析实时流量确定是否存在用户之间的水平越权行为。

[0037] 需要说明的是,本说明书提供的行为检测方法在服务端采用实时检测的方式执行,用于对任意时刻的待检测流量数据进行检测分析,从而实现及时确定越权行为的感知和防护,以避免服务端泄露数据和资源。

[0038] 进一步的,考虑到目标业务涉及到的流量数据覆盖维度较多,而每个维度并不是都会涉及到敏感数据,如果针对目标业务的全局流量进行检测,会消耗更多的计算资源和时间,因此为了能够高效且精准的检测异常行为,可以结合目标业务的历史流量数据确定关联敏感数据的维度,以该维度为基础进行每次检测前的流量数据过滤,本实施例中,具体实现方式如下:

[0039] 获取所述目标业务的历史流量数据;在所述历史流量数据中确定关联用户资源的资源访问数据,并基于所述资源访问数据生成基准访问信息;获取所述目标业务对应的初始流量数据;在所述初始流量数据中筛选出关联所述基准访问信息的流量数据,作为所述待检测流量数据。

[0040] 具体的,历史流量数据具体是指目标业务在当前检测前的任意时间区间对应的流

量数据,用于分析关联用户私有资源的访问数据;相应的,用户资源即为对应用户的私有资源,资源内容包括但不限于图像、文字、音频、交易信息等;相应的,资源访问数据具体是指历史流量数据中,关联用户资源的访问数据,资源访问数据由url、参数及参数值组成,通过资源访问数据能够访问用户的私有资源。相应的,基准访问信息具体是指针对资源访问数据生成的标记信息,用于标记流量中关联用户私有资源的描述信息,通过基准访问信息可以在流量数据中确定关联用户私有资源的访问数据,以方便后续结合这部分访问数据完成越权行为的检测和确认。相应的,初始流量数据具体是指当前时刻目标业务对应的全量实时流量。

[0041] 基于此,为了能够在大量的流量数据中筛选出因为水平越权行为导致数据泄露的基准访问信息,可以先获取目标业务的历史流量数据,之后在历史流量数据中确定关联用户资源的资源访问数据,也就是说,从历史流量数据中筛选出涉及用户私有资源的流量数据为资源访问数据;此后可以结合资源访问数据生成基准访问信息,以明确流量数据中有哪些访问数据是关联用户私有资源的。

[0042] 在确定基准访问信息后,若获取到关联目标业务的初始流量数据,即实时流量,可以按照基准访问信息对初始流量数据进行过滤,从而得到关联基准访问信息的流量数据,将其作为待检测流量数据,进行本次的水平越权行为的检测即可。

[0043] 具体实施时,可以采集一段历史时间内的http流量,通过http请求的cookie中的会话标识,可以获取每个用户对应的ID,将请求中的url、所有参数名以及参数值拼接后进行哈希运算,即可得到每个用户ID对应的唯一哈希值;基于该特性,可以明确若每个哈希值仅对应一个用户ID,则表明哈希运算前的url、所有参数名以及参数值为对应该ID所属用户访问私有资源的访问数据。也就是说,若某个url的所有历史流量中每个哈希值唯一对应一个用户ID,则确定该url请求的资源为用户自己对应的私有资源。

[0044] 在此基础上,在历史时间内的http流量中标记关联用户私有资源的url时,可以选择与用户ID或者私有资源关联的访问数据,结合这部分访问数据确定关联私有资源的url。当获取到实时流量后,可以基于标记出的url在实时流量中确定访问用户私有资源的流量,以方便后续进行水平越权行为的分析。

[0045] 需要说明的是,基准访问信息的确定可以在获取初始流量数据之前的任意时刻完成,本实施例在此不作任何限定。

[0046] 综上,通过结合历史流量数据整理出基准访问信息,并以基准访问信息为基础在后续的越权行为检测过程中,可以在实时流量中精准的筛选出关联用户私有资源的访问数据,并以此为基础进行水平越权行为的检测,可以有效减少处理的数据量,从而实现在更短的时间内完成越权行为检测,以避免出现遗漏问题。

[0047] 步骤S204,在所述待检测流量数据中确定用户标识,以及所述用户标识关联的访问数据。

[0048] 具体的,在上述获取到关联目标业务的待检测流量数据后,进一步的,考虑到待检测流量数据中包含大量的访问请求和反馈内容,因此为了能够完成对每个用户是否存在水平越权行为的检测,可以在待检测流量中确定每个用户的用户标识,以及每个用户标识关联的访问数据,方便后续结合访问数据和访问标识完成每个用户是否存在水平越权行为的检测。

[0049] 其中，用户标识具体是指参与目标业务的用户所具有的唯一标识，用于表征用户身份；相应的，访问数据具体是指每个用户标识对应的url数据、参数名数据和参数值数据等组成的，且用户标识与用户数据具有的关联性，是指每个用户标识关联的所有访问数据；正常情况下，每个用户标识对应一个访问数据；如果某个用户存在水平越权行为，则会发生该用户使用其他用户的标识进行私有资源的访问，此时就会出现多个用户标识对应一个访问数据，以此即可判定越权行为的发生。

[0050] 进一步的，在确定用户标识及其关联的访问数据时，考虑到该内容是确定用户是否存在水平越权行为的基础，因此需要保证用户标识和访问数据的准确关联性，因此可以结合会话标识和解析的方式实现，本实施例中，具体实现方式如步骤S2042至步骤S2044。

[0051] 步骤S2042，在所述待检测流量数据对应的用户信息文件中提取会话标识，并确定所述会话标识对应的所述用户标识。

[0052] 步骤S2044，对所述待检测流量数据进行解析，根据解析结果生成所述用户标识关联的所述访问数据。

[0053] 具体的，用户信息文件具体是指待检测流量数据中，实时流量数据请求cookie对应的文件，用于存储用户的用户标识；相应的，会话标识具体是指cookie文件中存储的标识，且会话标识与用户标识具有一一对应关系。

[0054] 基于此，在获取到待检测流量数据后，可以先确定待检测流量数据对应的用户信息文件，之后在用户信息文件中确定会话标识，以根据会话标识确定待检测流量数据涉及到的全部用户中，每个用户对应的用户标识；同时为了能够针对每个用户标识对应的用户进行水平越权行为的检测，可以对待检测流量数据进行解析，从而根据解析结果确定每个用户标识关联的访问数据，方便后续进行使用。

[0055] 需要说明的是，此时得到的用户标识与访问数据具有关联性，表征某个用户使用当前这个用户标识，通过访问数据对应的相关参数，读取该用户标识对应的私有资源，这一行为可能是用户标识所属的用户完成，也可能是其他用户使用该用户的用户标识完成，因此需要在得到用户标识关联的访问数据后，进行相关的检测处理操作。

[0056] 综上，通过结合待检测流量数据得到用户标识和访问数据，实现在数据分析阶段可以关联用户标识和访问数据，从而方便后续可以按照两者之间的关联性完成水平越权行为的检测，以保证检测精度。

[0057] 更进一步的，在解析待检测流量数据进行访问数据确定时，实则是结合访问数据中不同维度的数据组成，本实施例中，具体实现方式如下：

[0058] 对所述待检测流量数据进行解析，获得所述用户标识关联的访问地址、访问参数信息以及访问参数值；通过对所述访问地址、所述访问参数信息和所述访问参数值进行拼接，获得所述用户标识关联的所述访问数据。

[0059] 具体的，访问地址具体是指实时流量中进行私有资源访问时使用的地址，即url；相应的，访问参数信息具体是指实时流量中请求中相关参数的名称；访问参数值即为各个相关参数的取值；相应的，对访问地址、访问参数信息和访问参数值进行拼接，具体是指将三者的相关信息拼接到一起，拼接形式可以是首尾拼接等，本实施例在此不作任何限定。

[0060] 基于此，在得到用户标识后，考虑到访问用户私有资源时，需要结合用户标识和相应的访问数据完成，才能够读取到每个用户标识对应的私有数据，因此对待检测流量数据

进行解析，可以获得用户标识关联的访问地址、访问参数信息以及访问参数值，而这部分信息是进行私有资源访问时的基础，此时可以将访问地址、访问参数信息和访问参数值进行拼接，以根据拼接结果得到用户标识关联的访问数据，在后续进行使用。

[0061] 沿用上例，基于采集的实时流量，确定关联标记的url的内容后，可以得到用户甲对应的ID为ID_A，使用urlA访问用户甲私有资源，其中，使用urlA访问用户甲私有资源需要使用ID_A；用户乙对应的ID为ID_B，使用urlB访问用户乙私有资源，其中，使用urlB访问用户乙私有资源需要使用ID_B；用户丙对应的ID为ID_C，使用urlA访问用户甲私有资源，其中，使用urlA访问用户甲私有资源需要使用ID_A；在得到该部分数据后，即可用于后续针对每个用户进行越权行为的检测。

[0062] 综上，通过结合多维度数据组成访问数据，可以保证在进行水平越权行为检测时，具有更高的精准度，从而可以快速准确的作出应对，以避免数据泄露，进一步降低损失。

[0063] 步骤S206，对所述访问数据进行哈希运算，获得所述用户标识对应的访问哈希值。

[0064] 具体的，在上述得到用户标识关联的访问数据后，为了能够提高水平越权行为的检测速度以及准确度，可以对用户标识关联的访问数据进行哈希运算，从而得到每个用户标识对应的访问哈希值，后续结合目标业务预设的行为检测策略和访问哈希值，即可确定每个用户标识的访问行为信息，进而可以在需要时进行管控，避免数据泄露。

[0065] 步骤S208，基于所述目标业务的行为检测策略和所述访问哈希值，确定所述用户标识的访问行为信息；其中，所述行为检测策略关联水平越权行为检测维度。

[0066] 具体的，在上述得到用户标识对应的访问哈希值后，进一步的，考虑到不同业务场景下需要结合不同的方式进行水平越权行为的检测，因此可以先确定目标业务关联的行为检测策略，之后再融入访问哈希值，从而实现确定用户标识的访问行为信息，以此对待检测流量中涉及到的全部用户标识都进行检测，即可确定当前时刻是否存在水平越权行为，以针对相应问题及时作出应对措施。如封禁地址、封禁账号或者关闭私有资源访问等处理，本实施例在此不作任何限定。其中，行为检测策略具体是指针对不同业务场景设置的策略，该策略受控于服务方的计算资源和存储资源，即服务方的存储资源和计算资源的充足度控制行为检测策略。相应的，访问行为信息具体是指确定用户标识关联的用户是否存在水平越权行为的描述信息；相应的，水平越权行为检测维度具体是指对用户进行水平越权行为检测的维度。

[0067] 进一步的，在目标业务所属的业务方满足资源调用条件的情况下，说明目标业务所属的业务方具有充足的计算资源和存储资源，此时为了能够快速的完成水平越权行为的检测，可以预先建立访问信息表，在访问信息表中记录历史访问哈希值和历史用户标识之间的映射关系，在得到实时流量后，可以读取访问信息表确定映射关系是否正确，本实施例中，具体实现方式如下：

[0068] 基于所述目标业务的行为检测策略确定访问信息表；根据所述访问哈希值查询所述访问信息表，根据查询结果确定所述用户标识的访问行为信息；其中，所述访问信息表记录历史访问哈希值和历史用户标识之间的映射关系。

[0069] 具体的，资源调用条件具体是指能够水平越权行为检测时所调用的条件，通过资源调用条件可以确定当前业务场景下能够调用的资源是否可以支持水平越权行为的检测。相应的，访问信息表具体是指记录参与目标业务的用户关联的用户标识和访问哈希值的信

息表，由于每个用户的用户标识唯一，且访问私有数据时的访问数据唯一，因此其对应的访问哈希值也是唯一的，因此可以基于历史流量数据整理出用户标识和访问哈希值的映射关系，将其存储到访问信息表，用于在使用时查询表，即可确定当前得到的访问哈希值与用户标识的关系是否为访问信息表中存储的关系，进而确定水平越权行为。相应的，历史访问哈希值具体是指根据历史访问数据哈希运算后得到的哈希值。

[0070] 基于此，在目标业务所属的业务方满足资源调用条件的情况下，说明业务方的存储和计算资源充足，因此可以利用存储和计算资源预先建立访问信息表，并记录历史用户标识和历史访问哈希值的映射关系。在目标业务进行行为检测时，可以基于目标业务的行为检测策略确定访问信息表。而由于访问哈希值与用户标识对应，而访问信息表中记录的是历史访问哈希值和历史用户标识的映射关系，且访问信息表中记录的内容是准确的；因此可以基于访问哈希值查询访问信息表，根据查询结果即可确定用户标识对应的访问行为信息。即根据查询结果可以确定访问信息表中存储的历史用户标识，通过将历史用户标识访问哈希值对应的用户标识进行比较，即可确定用户标识的行为信息。

[0071] 需要说明的是，访问信息表需要预先建立，且访问信息表中存储的映射关系均为准确的映射关系，以此为基础才能够保证后续的任意时刻进行水平越权行为检测时的准确性。此外，考虑到参与目标业务的用户可能随时更新，因此访问信息表也可以随着用户的更新而更新，以保证每次检测时，都可以覆盖全部参与目标业务的用户。

[0072] 综上，在业务方持有资源足够的情况下，为了能够保证检测精度和效率，可以结合访问信息表进行访问行为信息的确定，从而能够在较短的时间内对大量的用户标识进行检测，以保证目标业务对应的业务方，针对水平越权行为可以作出快速解决决定。

[0073] 更进一步的，在进行访问行为信息确定时，实则是基于访问信息表中存储的用户标识与访问哈希值对应的用户标识比对完成，本实施例中，具体实现方式如下：

[0074] 根据查询结果确定关联用户标识，在所述关联用户标识与所述用户标识相同的情况下，确定访问正常信息作为所述用户标识的访问行为信息；或者，

[0075] 根据查询结果确定关联用户标识，在所述关联用户标识与所述用户标识不相同的情况下，确定访问异常信息作为所述用户标识的访问行为信息；或者，

[0076] 根据查询结果确定所述访问信息表中不存在关联用户标识的情况下，基于所述用户标识和所述访问哈希值生成目标映射关系，并将所述目标映射关系记录至所述访问信息表。

[0077] 第一方面，在查询访问信息表确定关联用户标识，且关联用户标识与用户标识相同的情况下，说明此时访问数据对应的用户标识，即为访问私有资源的用户对应的标识，进一步说明该用户标识不存在越权行为，因此可以将访问正常信息作为用户标识对应的访问行为信息。

[0078] 第二方面，在查询访问信息表确定关联用户标识，且关联用户标识与用户标识不相同的情况下，说明此时访问数据对应的用户标识，并不是访问私有资源的用户对应的标识，进一步说明有其他用户使用私有资源对应的用户的标识进行访问，则此时说明使用该用户标识的用户存在水平越权行为，因此可以确定访问异常信息为访问行为信息，以方便后续针对用户标识进行封禁等处理，避免使用该用户标识继续进行私有资源的读取等操作。

[0079] 第三方面，在查询访问信息表确定其中不存在关联用户标识的情况下，说明当前访问数据及其对应的用户标识，所属的用户是第一次参与目标业务，这种情况下用户标识对应的用户不可能存在水平越权行为，因此可以基于访问哈希值和用户标识创建目标映射关系，并将目标映射关系写入访问信息表，实现将新用户的信息存储到访问信息表，以用于后续的使用。

[0080] 沿用上例，通过对urlA为url:example.com/test?a＝123&b＝abc，采用sha256算法对urlA进行哈希运算，得到urlA对应的hash字符串A，同理，对urlB进行哈希运算，得到urlB对应的hash字符串B，此时可以确定实时流量中，hash字符串A与ID_A对应，hash字符串B与ID_B对应。

[0081] 进一步的，基于hash字符串A和B查询预先建立的访问信息表，根据查询结果确定hash字符串A在历史流量中对应的用户标识为ID_A，根据查询结果确定hash字符串B在历史流量中对应的用户标识为ID_B，通过将查询到的用户标识与实时流量中访问数据对应的用户标识进行比对，根据比对结果确定用户甲和用户乙均为正常的私有资源访问。而用户丙对应的ID_C与基于urlA对应的哈希值查询到的ID不一致，确定用户丙存在水平越权行为。

[0082] 此外，当根据hash字符串查询表未得到用户标识的情况下，说明当前表中不存在这一用户的相关映射关系，因此可以基于hash字符串和访问数据对应的用户标识组成新的映射关系，并将其写入到表中，以方便后续的处理阶段使用。

[0083] 实际应用中，在确定存在水平越权行为的用户标识后，考虑到检测行为发生在基于请求反馈私有资源前，因此可以对存在越权行为的用户标识进行封禁，或者临时关停目标业务，以避免造成私有资源的访问成功，而造成的数据泄露。

[0084] 本说明书提供的行为检测方法，为了能够提前感知越权行为并作出防护，可以在获取目标业务对应的待检测流量数据后，在待检测流量数据中确定用户标识，以及与用户标识关联的访问数据，之后对访问数据进行哈希运算，得到用户标识对应的访问哈希值，此时实现了针对每条访问数据生成唯一对应关系的哈希值，以方便后续能够进行访问行为检测。此后通过结合目标业务的行为检测策略和访问哈希值，实现在针对访问数据反馈私有资源前，完成对用户标识的访问行为信息的确定，可以达到提前感知越权行为和防护的效果，以避免数据泄露而造成的损失。

[0085] 与上述实施例相对应，本说明书还提供了另一种行为检测方法，图3示出了根据本说明书一个实施例提供的另一种行为检测方法的流程图，具体包括以下步骤。

[0086] 步骤S302，获取目标业务对应的待检测流量数据。

[0087] 本说明书提供的行为检测方法应用于网站的行为检测过程，该方法应用于网站所属的服务端，由服务端根据实时采集到的流量数据进行水平越权行为检测，且在检测完成后可以及时熔断，或者对异常行为用户的账号进行封禁等操作，本实施例在此不作任何限定。

[0088] 具体的，目标业务具体是指能够通过使用网站进行资源访问、读取和/或下载等操作的业务，且访问、读取和/或下载等操作涉及到的资源至少包括每个用户所对应的私有资源。即目标业务会涉及到每个用户私有资源的访问、读取和/或下载等操作，该过程可能会发生用户之间的水平越权行为。相应的，待检测流量数据具体是指目标业务在当前时刻所对应的实时流量，用于实现后续可以通过分析实时流量确定是否存在用户之间的水平越权

行为发生。

[0089] 需要说明的是，本说明书提供的行为检测方法在服务端采用实时检测的方式执行，用于对任意时刻的待检测流量数据进行检测分析，从而实现及时确定越权行为的感知和防护，以避免服务端泄露数据和资源。

[0090] 步骤S304，在所述待检测流量数据中确定用户标识，以及所述用户标识关联的访问数据。

[0091] 具体的，在上述获取到关联目标业务的待检测流量数据后，进一步的，考虑到待检测流量数据中包含大量的访问请求和反馈内容，因此为了能够完成对每个用户是否存在水平越权行为的检测，可以在待检测流量中确定每个用户的用户标识，以及每个用户标识关联的访问数据，方便后续结合访问数据和访问标识完成每个用户是否存在水平越权行为的检测。

[0092] 其中，用户标识具体是指参与目标业务的用户所具有的唯一标识，用于表征用户身份；相应的，访问数据具体是指每个用户标识对应的url数据、参数名数据和参数值数据等组成的，且用户标识与用户数据具有的关联性，是指每个用户标识关联的所有访问数据；正常情况下，每个用户标识对应一个访问数据；如果某个用户存在水平越权行为，则会发生该用户使用其他用户的标识进行私有资源的访问，此时就会出现多个用户标识对应一个访问数据，以此即可判定越权行为的发生。

[0093] 步骤S306，对所述访问数据进行哈希运算，获得所述用户标识对应的访问哈希值。

[0094] 具体的，在上述得到用户标识关联的访问数据后，为了能够提高水平越权行为的检测速度以及准确度，可以对用户标识关联的访问数据进行哈希运算，从而得到每个用户标识对应的访问哈希值，后续结合目标业务预设的行为检测策略和访问哈希值，即可确定每个用户标识的访问行为信息，进而可以在需要时进行管控，避免数据泄露。

[0095] 需要说明的是，本实施例提供的另一种行为检测方法与上述实施例提供的行为检测方法相对应，其中步骤S302至步骤S306的描述内容，均可参见上述实施例中相同或相应的描述内容，在此不作过多赘述。此外，本实施例提供的与上述实施例相同描述的内容，也均可参见上述实施例，本实施例在此不作任何限定。

[0096] 步骤S308，在所述目标业务所属的业务方不满足资源调用条件的情况下，根据所述待检测流量数据，确定预设时间区间内所述访问哈希值对应的用户标识数量。

[0097] 具体的，在上述得到用户标识对应的访问哈希值后，进一步的，考虑到不同业务场景下需要结合不同的方式进行水平越权行为的检测，因此可以先确定目标业务关联的行为检测策略，之后再融入访问哈希值，从而实现确定用户标识的访问行为信息，以此对待检测流量中涉及到的全部用户标识都进行检测，即可确定当前时刻是否存在水平越权行为，以针对相应问题及时作出应对措施。如封禁地址、封禁账号或者关闭私有资源访问等处理，本实施例在此不作任何限定。

[0098] 基于此，在确定不满足资源调用条件的情况下，可以先根据待检测流量数据，确定预设时间区间内访问哈希值对应的用户标识数量，之后根据用户标识数量进行访问行为信息的确定。其中，预设时间区间具体是指通过用户标识数量的时间，该时间区间的长度可以根据实际应用场景设定，比如5分钟、10分钟等，本实施例在此不作任何限定。

[0099] 也就是说，在目标业务所属的业务方不满足资源调用条件的情况下，说明目标业

务所属的业务方具有的计算资源和存储资源不充足，此时若再调用部分存储资源和计算资源用于进行水平越权行为的检测，可能会造成业务方的资源调用压力，因此针对不满足条件的情况，可以在得到用户标识对应的访问哈希值后，采用统计访问哈希值与用户标识数量对应关系的方式实现检测。即，当存在水平越权行为时，同一个访问数据可能会对应至少两个用户标识，用于访问不同用户的私有资源，这个时候就说明有用户在恶意操作，因此可以采用这一机制进行越权行为检测。

[0100] 进一步的，在确定该用户标识数量的过程中，考虑到用户标识关联访问数据，而访问数据经过哈希运算得到访问哈希值，因此可以基于访问数据完成用户标识数量的统计，本实施例中，具体实现方式如下：

[0101] 根据所述待检测流量数据，确定预设时间区间内所述访问数据对应的访问用户标识；统计所述访问用户标识对应的标识数量，作为所述访问哈希值对应的用户标识数量。

[0102] 基于此，待检测流量数据中包含预设时间段内的全部流量，因此可以通过分析待检测数据流量，确定预设时间区间内访问数据对应的访问用户标识；通常情况下，每个访问数据应该对应一个访问用户标识，因为每个用户仅会通过自己的用户标识进行私有资源的访问，如果超过就可能存在越权行为。因此可以统计访问用户标识对应的标识数量，而由于访问数据经过哈希计算得到访问哈希值，因此可以根据标识数据确定访问哈希值对应的用户标识数量，以方便后续进行数量比较，从而确定是否存在于越权行为。

[0103] 例如，用户甲对应的ID为ID_A，使用urlA访问用户甲私有资源，其中，使用urlA访问用户甲私有资源需要使用ID_A；用户乙对应的ID为ID_B，使用urlB访问用户乙私有资源，其中，使用urlB访问用户乙私有资源需要使用ID_B；用户丙对应的ID为ID_C，使用urlA访问用户甲私有资源，其中，使用urlA访问用户甲私有资源需要使用ID_A。

[0104] 通过对urlA为url:example.com/test?a＝123&b＝abc，采用sha256算法对urlA进行哈希运算，得到urlA对应的hash字符串A，同理，对urlB进行哈希运算，得到urlB对应的hash字符串B，此时可以确定实时流量中，hash字符串A与ID_A和ID_C对应，hash字符串B与ID_B对应。

[0105] 进一步的，通过统计10分钟内每个访问数据对应的访问用户标识，确定urlA对应ID_A和ID_C，urlB对应ID_B，进而确定hash字符串A对应的用户标识数量为2，确定hash字符串B对应的用户标识数量为1，以方便后续结合用户标识数量进行水平越权行为的检测。

[0106] 综上，通过统计访问数据用户标识数据的方式，确定访问哈希值对应的用户标识数量，从而方便后续可以通过分析预设时间段内的用户标识数量完成水平越权行为分析，从而保证越权行为分析的准确度。

[0107] 步骤S310，基于所述行为检测策略对所述用户标识数量进行检测，根据检测结果确定所述用户标识的访问行为信息。

[0108] 具体的，在上述得到用户标识数量后，进一步的，可以基于行为检测策略对用户标识数量进行检测，从而分析数量是否达到上限，以根据检测结果确定用户标识的访问行为信息。其中，访问行为信息具体是指确定用户标识关联的用户是否存在水平越权行为的描述信息；

[0109] 进一步的，在基于用户标识数量分析用户是否存在水平越权行为时，可以结合预设的数量阈值实现，通过比较数量阈值的方式完成，本实施例中，具体实现方式如下：

[0110] 基于所述行为检测策略确定所述用户标识数量大于预设数量阈值的情况下，确定访问异常信息作为所述用户标识的访问行为信息；或者，基于所述行为检测策略确定所述用户标识数量小于等于预设数量阈值的情况下，确定访问正常信息作为所述用户标识的访问行为信息。

[0111] 具体实施时，预设数量阈值可以根据实际应用场景进行设定，例如1，2等数值，本实施例在此不作任何限定。

[0112] 第一方面，基于行为检测检测策略确定用户标识数量大于预设数量阈值的情况下，说明此时存在水平越权行为，为避免造成损失，可以将访问异常信息作为用户标识的访问行为信息。

[0113] 第二方面，基于行为检测检测策略确定用户标识数量小于等于预设数量阈值的情况下，说明此时并不存在水平越权行为，因此可以将访问正常信息作为用户标识对应的访问行为信息。

[0114] 沿用上例，根据统计结果确定hash字符串A对应的用户标识数量为2，确定hash字符串B对应的用户标识数量为1，而预设数量阈值为1，通过比较确定hash字符串A对应的用户标识数量为2大于1，进而确定存在水平越权行为。

[0115] 综上，通过采用数量阈值比较的方式对访问行为信息的确定，可以保证在较短的时间内完成水平越权行为的检测，从而提高检测精度，同时能够降低计算资源的消耗。

[0116] 此外，考虑到通过一次检测可能存在检测精度较低的风险，且业务方也需要判定水平越权行为是否发生，从而减少损失，因此在访问行为信息确定后，可以进行越权是否成功的检测，本实施例中，具体实现方式如下：

[0117] 获取所述访问数据对应每个访问用户标识的访问反馈结果；对每个访问用户标识的访问反馈结果分别进行哈希运算，获得每个访问用户标识对应的反馈哈希值；将每个访问用户标识对应的反馈哈希值进行比较，根据比较结果确定所述用户标识的异常行为结果。

[0118] 具体的，访问反馈结果具体是指针对访问数据向访问用户标识反馈的内容，包括但不限于关联访问用户标识的私有资源、信息等。相应的，反馈哈希值具体是指对反馈结果进行哈希运算后得到的哈希值，该哈希运算可以采用与访问数据的哈希运算相同的方式，本实施例在此不作任何限定。相应的，异常行为结果具体是指确定越权行为是否已经成功的结果。

[0119] 基于此，为了避免造成过多的损失，可以先确定存在水平越权行为后，获取访问数据每个访问用户标识对应的访问反馈结果。之后对访问反馈结果进行哈希运算，得到每个访问用户标识对应的反馈哈希值，通过将各个访问用户标识之间的反馈哈希值进行比较，即可确定用户标识对应的异常行为结果。该结果包括成功或者不成功。用于表示水平越权行为是否成功。

[0120] 沿用上例，在确定hash字符串A对应ID_A和ID_C后，可以对基于ID_A反馈的私有资源进行哈希运算，得到hash字符串A1，以及对ID_C反馈的私有资源进行哈希运算，得到hash字符串C1，若hash字符串A1和hash字符串C1相等，表示水平越权行为成功，反之则表示不成功。

[0121] 通过采用比较反馈哈希值的方式进行水平越权行为成功与失败的检测，可以进一

步确定是否发生私有资源泄露的问题，从而可以及时作出响应，以避免造成过多的损失。

[0122] 综上所述，为了能够提前感知越权行为并作出防护，可以在获取目标业务对应的待检测流量数据后，在待检测流量数据中确定用户标识，以及与用户标识关联的访问数据，之后对访问数据进行哈希运算，得到用户标识对应的访问哈希值，此时实现了针对每条访问数据生成唯一对应关系的哈希值，以方便后续能够进行访问行为检测。此后通过结合目标业务的行为检测策略和访问哈希值，实现在针对访问数据反馈私有资源前，完成对用户标识的访问行为信息的确定，可以达到提前感知越权行为和防护的效果，以避免数据泄露而造成的损失。

[0123] 与上述方法实施例相对应，本说明书还提供了行为检测装置实施例，图4示出了本说明书一个实施例提供的一种行为检测装置的结构示意图。如图4所示，该装置包括：

[0124] 获取数据模块402，被配置为获取目标业务对应的待检测流量数据；

[0125] 确定标识模块404，被配置为在所述待检测流量数据中确定用户标识，以及所述用户标识关联的访问数据；

[0126] 哈希运算模块406，被配置为对所述访问数据进行哈希运算，获得所述用户标识对应的访问哈希值；

[0127] 确定信息模块408，被配置为基于所述目标业务的行为检测策略和所述访问哈希值，确定所述用户标识的访问行为信息；其中，所述行为检测策略关联水平越权行为检测维度。

[0128] 一个可选的实施例中，所述装置，还包括：

[0129] 生成信息模块，被配置为获取所述目标业务的历史流量数据；在所述历史流量数据中确定关联用户资源的资源访问数据，并基于所述资源访问数据生成基准访问信息；

[0130] 相应的，所述获取数据模块402进一步被配置为：

[0131] 获取所述目标业务对应的初始流量数据；在所述初始流量数据中筛选出关联所述基准访问信息的流量数据，作为所述待检测流量数据。

[0132] 一个可选的实施例中，所述确定标识模块404进一步被配置为：

[0133] 在所述待检测流量数据对应的用户信息文件中提取会话标识，并确定所述会话标识对应的所述用户标识；对所述待检测流量数据进行解析，根据解析结果生成所述用户标识关联的所述访问数据。

[0134] 一个可选的实施例中，所述确定标识模块404进一步被配置为：

[0135] 对所述待检测流量数据进行解析，获得所述用户标识关联的访问地址、访问参数信息以及访问参数值；通过对所述访问地址、所述访问参数信息和所述访问参数值进行拼接，获得所述用户标识关联的所述访问数据。

[0136] 一个可选的实施例中，在所述目标业务所属的业务方满足资源调用条件的情况下，所述确定信息模块408进一步被配置为：

[0137] 基于所述目标业务的行为检测策略确定访问信息表；根据所述访问哈希值查询所述访问信息表，根据查询结果确定所述用户标识的访问行为信息；其中，所述访问信息表记录历史访问哈希值和历史用户标识之间的映射关系。

[0138] 一个可选的实施例中，所述确定信息模块408进一步被配置为：

[0139] 根据查询结果确定关联用户标识，在所述关联用户标识与所述用户标识相同的情

况下，确定访问正常信息作为所述用户标识的访问行为信息；或者，根据查询结果确定关联用户标识，在所述关联用户标识与所述用户标识不相同的情况下，确定访问异常信息作为所述用户标识的访问行为信息；或者，根据查询结果确定所述访问信息表中不存在关联用户标识的情况下，基于所述用户标识和所述访问哈希值生成目标映射关系，并将所述目标映射关系记录至所述访问信息表。

[0140] 一个可选的实施例中，在所述目标业务所属的业务方不满足资源调用条件的情况下，所述确定信息模块408进一步被配置为：

[0141] 根据所述待检测流量数据，确定预设时间区间内所述访问哈希值对应的用户标识数量；基于所述行为检测策略对所述用户标识数量进行检测，根据检测结果确定所述用户标识的访问行为信息。

[0142] 一个可选的实施例中，所述确定信息模块408进一步被配置为：

[0143] 根据所述待检测流量数据，确定预设时间区间内所述访问数据对应的访问用户标识；统计所述访问用户标识对应的标识数量，作为所述访问哈希值对应的用户标识数量。

[0144] 一个可选的实施例中，所述确定信息模块408进一步被配置为：

[0145] 基于所述行为检测策略确定所述用户标识数量大于预设数量阈值的情况下，确定访问异常信息作为所述用户标识的访问行为信息；或者，基于所述行为检测策略确定所述用户标识数量小于等于预设数量阈值的情况下，确定访问正常信息作为所述用户标识的访问行为信息。

[0146] 一个可选的实施例中，所述装置，还包括：

[0147] 异常行为检测模块，被配置为获取所述访问数据对应每个访问用户标识的访问反馈结果；对每个访问用户标识的访问反馈结果分别进行哈希运算，获得每个访问用户标识对应的反馈哈希值；将每个访问用户标识对应的反馈哈希值进行比较，根据比较结果确定所述用户标识的异常行为结果。

[0148] 本说明书提供的行为检测装置，为了能够提前感知越权行为并作出防护，可以在获取目标业务对应的待检测流量数据后，在待检测流量数据中确定用户标识，以及与用户标识关联的访问数据，之后对访问数据进行哈希运算，得到用户标识对应的访问哈希值，此时实现了针对每条访问数据生成唯一对应关系的哈希值，以方便后续能够进行访问行为检测。此后通过结合目标业务的行为检测策略和访问哈希值，实现在针对访问数据反馈私有资源前，完成对用户标识的访问行为信息的确定，可以达到提前感知越权行为和防护的效果，以避免数据泄露而造成的损失。

[0149] 上述为本实施例的一种行为检测装置的示意性方案。需要说明的是，该行为检测装置的技术方案与上述的行为检测方法的技术方案属于同一构思，行为检测装置的技术方案未详细描述的细节内容，均可以参见上述行为检测方法的技术方案的描述。

[0150] 图5示出了根据本说明书一个实施例提供的一种计算设备500的结构框图。该计算设备500的部件包括但不限于存储器510和处理器520。处理器520与存储器510通过总线530相连接，数据库550用于保存数据。

[0151] 计算设备500还包括接入设备540，接入设备540使得计算设备500能够经由一个或多个网络560通信。这些网络的示例包括公用交换电话网(PSTN)、局域网(LAN)、广域网(WAN)、个域网(PAN)或诸如因特网的通信网络的组合。接入设备540可以包括有线或无线的

任何类型的网络接口(例如,网络接口卡(NIC))中的一个或多个,诸如IEEE802.11无线局域网(WLAN)无线接口、全球微波互联接入(Wi-MAX)接口、以太网接口、通用串行总线(USB)接口、蜂窝网络接口、蓝牙接口、近场通信(NFC)接口,等等。

[0152] 在本说明书的一个实施例中,计算设备500的上述部件以及图5中未示出的其他部件也可以彼此相连接,例如通过总线。应当理解,图5所示的计算设备结构框图仅仅是出于示例的目的,而不是对本说明书范围的限制。本领域技术人员可以根据需要,增添或替换其他部件。

[0153] 计算设备500可以是任何类型的静止或移动计算设备,包括移动计算机或移动计算设备(例如,平板计算机、个人数字助理、膝上型计算机、笔记本计算机、上网本等)、移动电话(例如,智能手机)、可佩戴的计算设备(例如,智能手表、智能眼镜等)或其他类型的移动设备,或者诸如台式计算机或PC的静止计算设备。计算设备500还可以是移动式或静止式的服务器。

[0154] 其中,处理器520用于执行如下计算机可执行指令,该计算机可执行指令被处理器执行时实现上述行为检测方法的步骤。

[0155] 上述为本实施例的一种计算设备的示意性方案。需要说明的是,该计算设备的技术方案与上述的行为检测方法的技术方案属于同一构思,计算设备的技术方案未详细描述的细节内容,均可以参见上述行为检测方法的技术方案的描述。

[0156] 本说明书一实施例还提供一种计算机可读存储介质,其存储有计算机可执行指令,该计算机可执行指令被处理器执行时实现上述行为检测方法的步骤。

[0157] 上述为本实施例的一种计算机可读存储介质的示意性方案。需要说明的是,该存储介质的技术方案与上述的行为检测方法的技术方案属于同一构思,存储介质的技术方案未详细描述的细节内容,均可以参见上述行为检测方法的技术方案的描述。

[0158] 本说明书一实施例还提供一种计算机程序,其中,当所述计算机程序在计算机中执行时,令计算机执行上述行为检测方法的步骤。

[0159] 上述为本实施例的一种计算机程序的示意性方案。需要说明的是,该计算机程序的技术方案与上述的行为检测方法的技术方案属于同一构思,计算机程序的技术方案未详细描述的细节内容,均可以参见上述行为检测方法的技术方案的描述。

[0160] 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。

[0161] 所述计算机指令包括计算机程序代码,所述计算机程序代码可以为源代码形式、对象代码形式、可执行文件或某些中间形式等。所述计算机可读介质可以包括:能够携带所述计算机程序代码的任何实体或装置、记录介质、U盘、移动硬盘、磁碟、光盘、计算机存储器、只读存储器(ROM,Read-OnlyMemory)、随机存取存储器(RAM,RandomAccessMemory)、电载波信号、电信信号以及软件分发介质等。需要说明的是,所述计算机可读介质包含的内容可以根据司法管辖区内立法和专利实践的要求进行适当的增减,例如在某些司法管辖区,根据立法和专利实践,计算机可读介质不包括电载波信号和电信信号。

[0162] 需要说明的是，对于前述的各方法实施例，为了简便描述，故将其都表述为一系列的动作组合，但是本领域技术人员应该知悉，本说明书实施例并不受所描述的动作顺序的限制，因为依据本说明书实施例，某些步骤可以采用其它顺序或者同时进行。其次，本领域技术人员也应该知悉，说明书中所描述的实施例均属于优选实施例，所涉及的动作和模块并不一定都是本说明书实施例所必须的。

[0163] 在上述实施例中，对各个实施例的描述都各有侧重，某个实施例中没有详述的部分，可以参见其它实施例的相关描述。

[0164] 以上公开的本说明书优选实施例只是用于帮助阐述本说明书。可选实施例并没有详尽叙述所有的细节，也不限制该发明仅为所述的具体实施方式。显然，根据本说明书实施例的内容，可作很多的修改和变化。本说明书选取并具体描述这些实施例，是为了更好地解释本说明书实施例的原理和实际应用，从而使所属技术领域技术人员能很好地理解和利用本说明书。本说明书仅受权利要求书及其全部范围和等效物的限制。

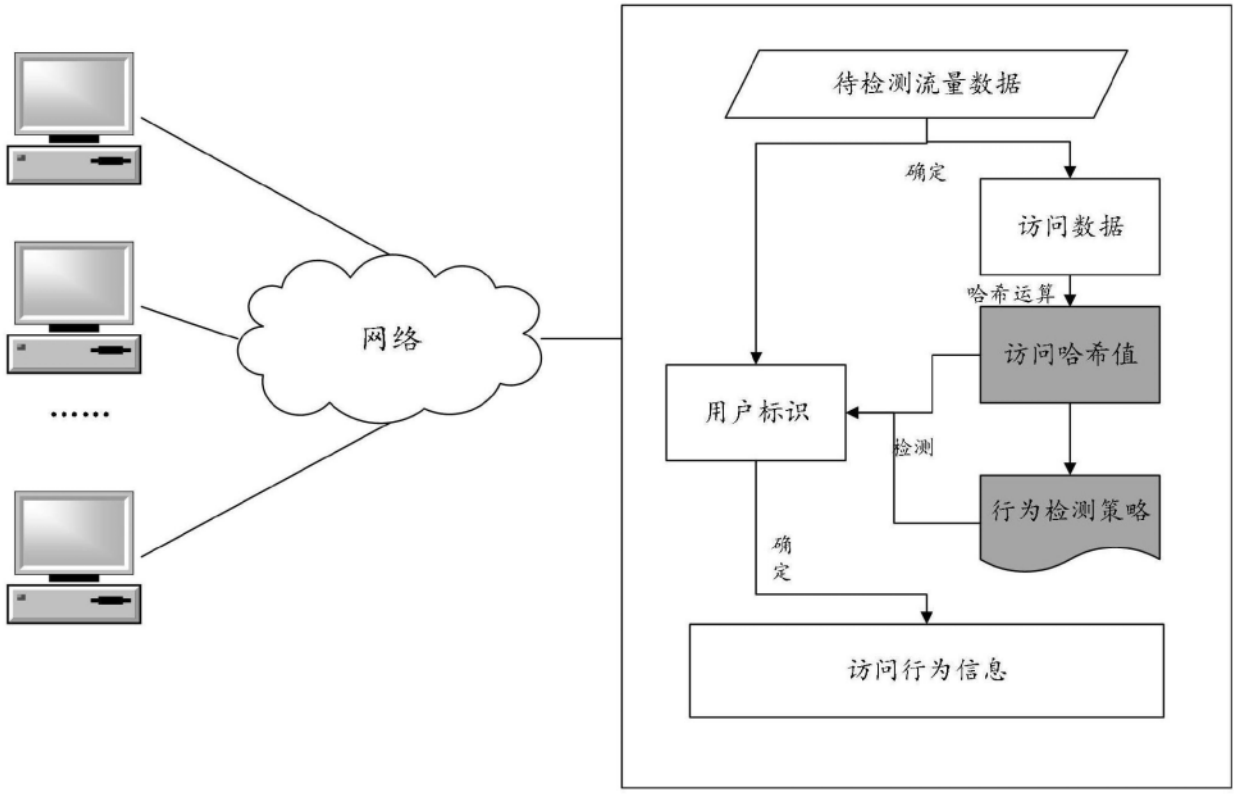

网络
.....
待检测流量数据
确定
访问数据
哈希运算
访问哈希值
用户标识
检测
行为检测策略
确定
访问行为信息

图1

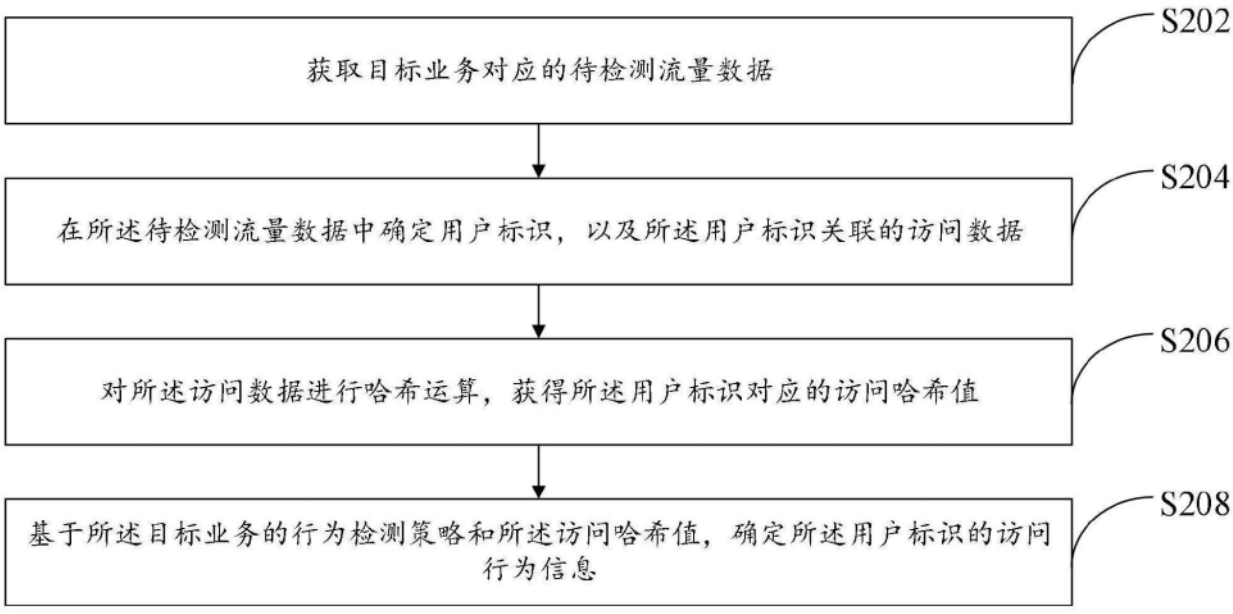

S202
获取目标业务对应的待检测流量数据
S204
在所述待检测流量数据中确定用户标识，以及所述用户标识关联的访问数据
S206
对所述访问数据进行哈希运算，获得所述用户标识对应的访问哈希值
S208
基于所述目标业务的行为检测策略和所述访问哈希值，确定所述用户标识的访问行为信息

图2

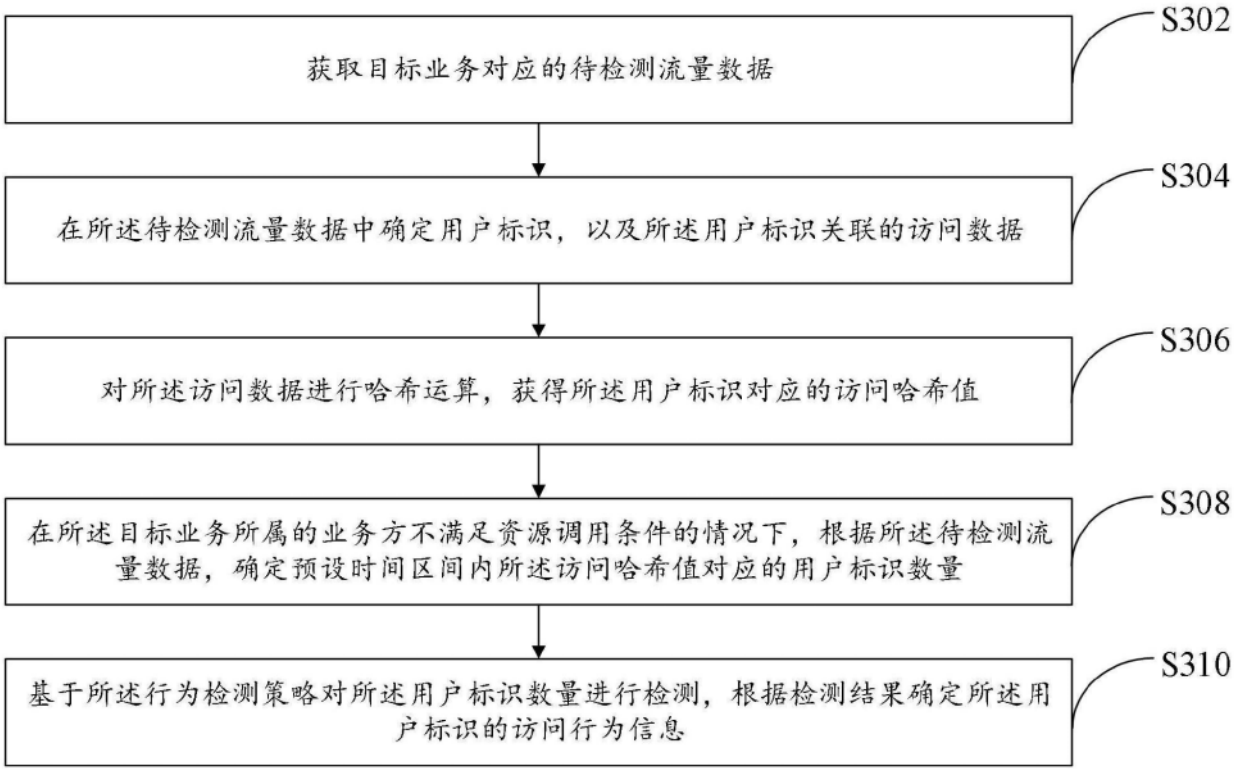

获取目标业务对应的待检测流量数据
S302
在所述待检测流量数据中确定用户标识，以及所述用户标识关联的访问数据
S304
对所述访问数据进行哈希运算，获得所述用户标识对应的访问哈希值
S306
在所述目标业务所属的业务方不满足资源调用条件的情况下，根据所述待检测流量数据，确定预设时间区间内所述访问哈希值对应的用户标识数量
S308
基于所述行为检测策略对所述用户标识数量进行检测，根据检测结果确定所述用户标识的访问行为信息
S310

图3

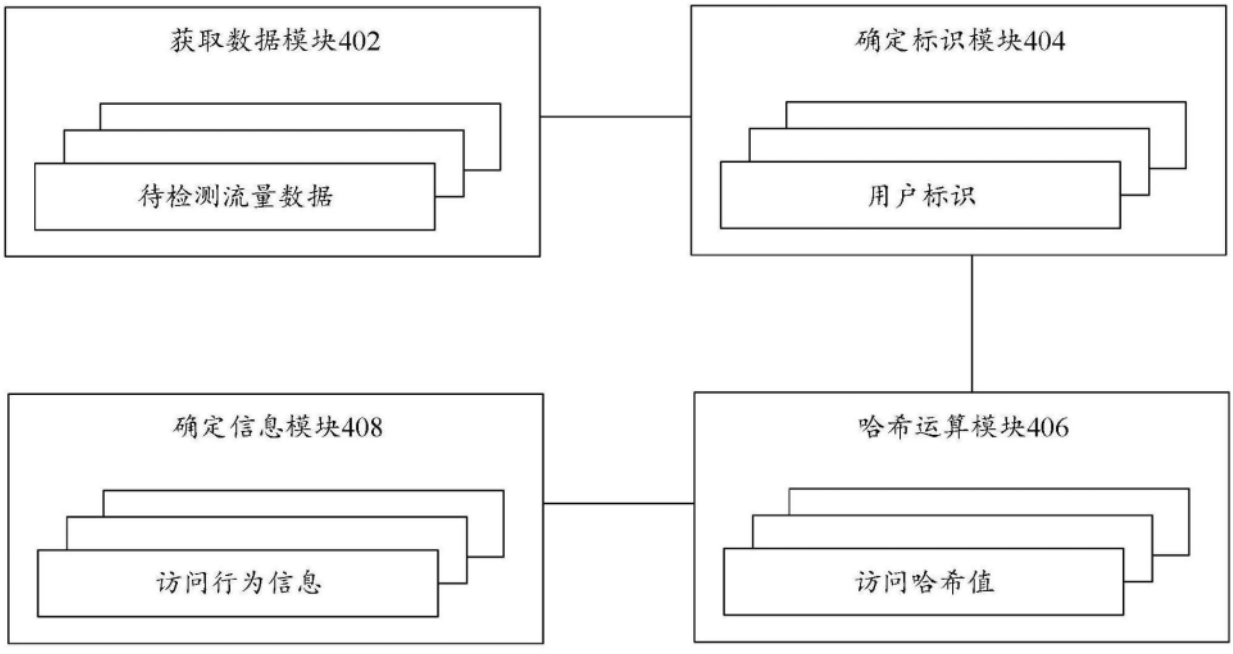

获取数据模块402
待检测流量数据
确定标识模块404
用户标识
确定信息模块408
访问行为信息
哈希运算模块406
访问哈希值

图4

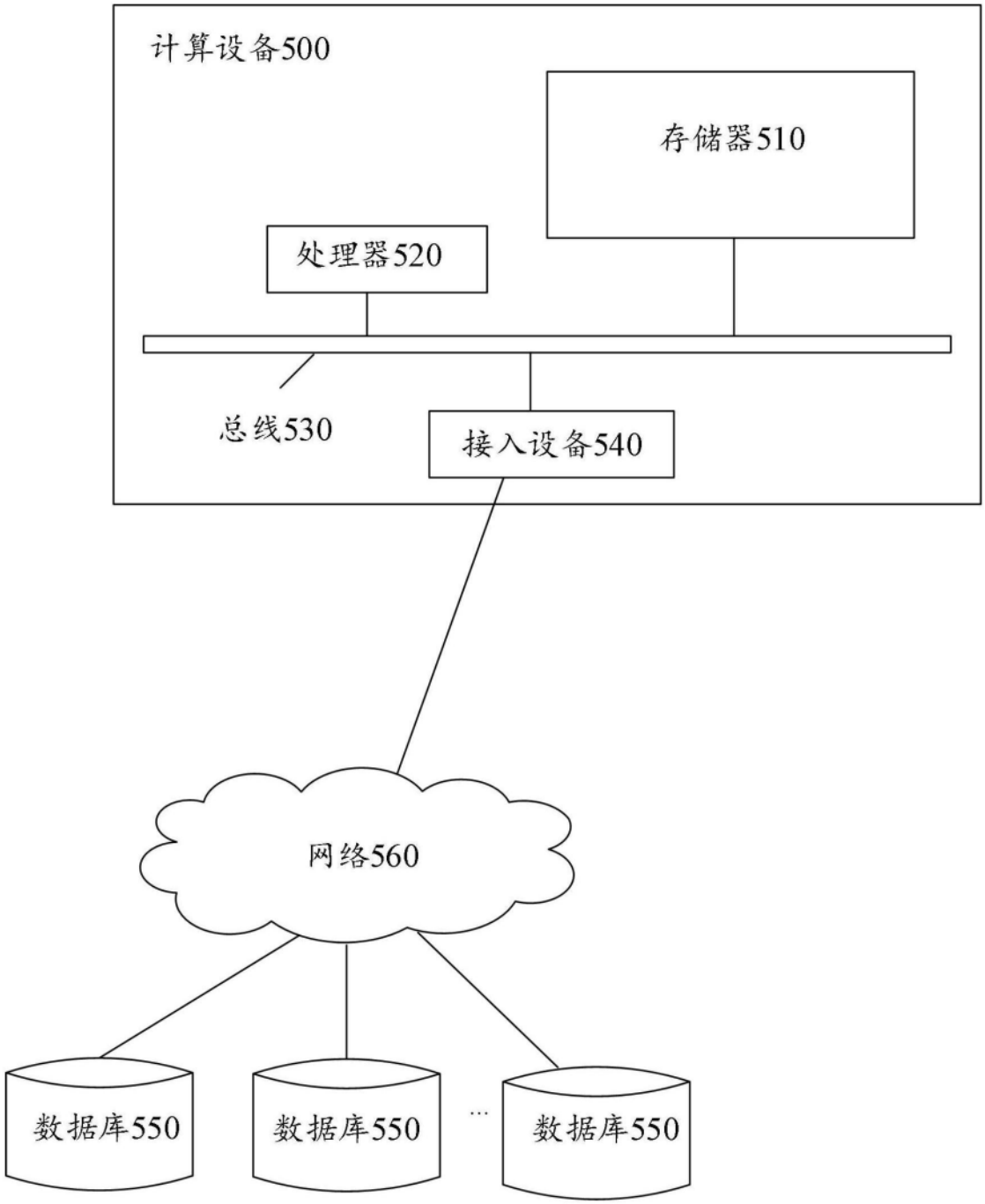

计算设备500
存储器510
处理器520
总线530
接入设备540
网络560
数据库550
数据库550
…
数据库550

图5