(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 116155597 A
(43)申请公布日 2023.05.23

(21)申请号 202310152466.2

(22)申请日 2023.02.22

(71)申请人 企查查科技有限公司
地址 215000 江苏省苏州市苏州工业园区东长路88号C1幢5层503室

(72)发明人 吴帅帅 温时豪 毕高威 沈耀杰 朱正亮

(74)专利代理机构 华进联合专利商标代理有限公司 44224
专利代理师 郭凤杰

(51)Int.Cl.
*H04L 9/40*(2022.01)
*G06F 16/951*(2019.01)
*G06F 16/953*(2019.01)
*G06F 9/54*(2006.01)

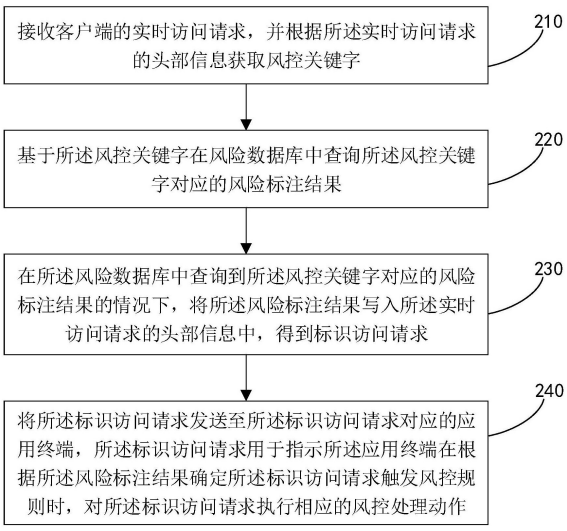
权利要求书2页 说明书12页 附图9页

(54)发明名称

# 访问请求的处理方法、装置及计算机设备

(57)摘要

本公开涉及网络信息技术领域，具体公开了一种访问请求的处理方法、装置及计算机设备，所述方法包括：接收客户端的实时访问请求，并根据所述实时访问请求的头部信息获取风控关键字；基于所述风控关键字在风险数据库中查询所述风控关键字对应的风险标注结果；在所述风险数据库中查询到所述风控关键字对应的风险标注结果的情况下，将所述风险标注结果写入所述实时访问请求的头部信息中，得到标识访问请求；将所述标识访问请求发送至所述标识访问请求对应的应用终端。本公开对爬虫识别和响应业务请求做了解耦处理；提高了爬虫识别和业务请求的识别准确率。




CN 116155597 A

1.一种访问请求的处理方法,其特征在于,所述方法包括:

接收客户端的实时访问请求,并根据所述实时访问请求的头部信息获取风控关键字;

基于所述风控关键字在风险数据库中查询所述风控关键字对应的风险标注结果;所述风险数据库用于存储风控关键字和风险标注结果的对应关系;

在所述风险数据库中查询到所述风控关键字对应的风险标注结果的情况下,将所述风险标注结果写入所述实时访问请求的头部信息中,得到标识访问请求;

将所述标识访问请求发送至所述标识访问请求对应的应用终端,所述标识访问请求用于指示所述应用终端在根据所述风险标注结果确定所述标识访问请求触发风控规则时,对所述标识访问请求执行相应的风控处理动作。

2.根据权利要求1所述的方法,其特征在于,所述方法还包括:

在所述风险数据库中未查询到所述风控关键字对应的风险标注结果的情况下,将所述实时访问请求推送至消息队列;

从所述消息队列中读取所述实时访问请求,按照预设的风险规则匹配所述实时访问请求的风控关键字,获得所述实时访问请求对应的风险标注结果;

将所述风险标注结果写入所述实时访问请求的头部信息中,得到所述标识访问请求;

将所述标识访问请求的风控关键字与所述风险标注结果存储至所述风险数据库。

3.根据权利要求1所述的方法,其特征在于,所述方法还包括:

按照设定的时间间隔获取历史访问请求,并获取所述历史访问请求的风控关键字;

按照预设的风险规则匹配所述历史访问请求的风控关键字,获得所述历史访问请求对应的风险标注结果;

将所述历史访问请求的风控关键字与所述历史访问请求对应的风险标注结果存储至所述风险数据库。

4.根据权利要求1所述的方法,其特征在于,所述应用终端在根据所述风险标注结果确定所述标识访问请求触发风控规则时,对所述标识访问请求执行相应的风控处理动作包括:

所述应用终端根据所述标识访问请求的风控关键字在风控规则数据库中查询所述风控关键字对应的风控规则;所述风控规则数据库用于存储风控关键字和风控规则的对应关系;

响应于在风控规则数据库中查询到所述风控关键字对应的风控规则,所述应用终端根据所述标识访问请求对应的风控规则向所述客户端返回风控指令,所述风控指令用于指示所述客户端执行所述风控处理动作。

5.根据权利要求4所述的方法,其特征在于,所述风控处理动作包括动态验证码验证动作、滑动验证码验证动作、封禁提示动作或强制登录动作中的一种或多种。

6.根据权利要求1所述的方法,其特征在于,所述标识访问请求还用于指示所述应用终端在根据所述风险标注结果确定所述标识访问请求未触发所述风控规则时,向所述客户端返回所述标识访问请求的请求结果。

7.根据权利要求6所述的方法,其特征在于,所述应用终端在根据所述风险标注结果确定所述标识访问请求未触发所述风控规则时,向所述客户端返回所述标识访问请求的请求结果包括:

所述应用终端根据所述标识访问请求的风控关键字在风控规则数据库中查询所述风控关键字对应的风控规则;所述风控规则数据库用于存储风控关键字和风控规则的对应关系;

响应于在风控规则数据库中未查询到所述风控关键字对应的风控规则,所述应用终端根据所述标识访问请求向所述客户端返回请求结果。

8.一种访问请求的处理装置,其特征在于,所述装置包括:

实时访问请求模块,用于接收客户端的实时访问请求,并根据所述实时访问请求的头部信息获取风控关键字;

风险查询模块,用于基于所述风控关键字在风险数据库中查询所述风控关键字对应的风险标注结果;所述风险数据库用于存储风控关键字和风险标注结果的对应关系;

标识访问请求模块,用于在所述风险数据库中查询到所述风控关键字对应的风险标注结果的情况下,将所述风险标注结果写入所述实时访问请求的头部信息中,得到标识访问请求;

请求处理模块,用于将所述标识访问请求发送至所述标识访问请求对应的应用终端,所述标识访问请求用于指示所述应用终端在根据所述风险标注结果确定所述标识访问请求触发风控规则时,对所述标识访问请求执行相应的风控处理动作。

9.一种计算机设备,包括存储器和处理器,所述存储器存储有计算机程序,其特征在于,所述处理器执行所述计算机程序时实现权利要求1至7中任一项所述的方法的步骤。

10.一种计算机可读存储介质,其上存储有计算机程序,其特征在于,所述计算机程序被处理器执行时实现权利要求1至7中任一项所述的方法的步骤。

# 访问请求的处理方法、装置及计算机设备

## 技术领域

[0001] 本公开涉及网络信息技术领域，特别是涉及一种访问请求的处理方法、装置及计算机设备。

## 背景技术

[0002] 随着网络的迅速发展，万维网成为大量信息的载体，同时网络信息的发布渠道和平台得到进一步的丰富，因此通用的搜索引擎面临着巨大的挑战，网络爬虫技术应运而生。网络爬虫是一个按照一定的规则自动提取网页的程序或脚本，它为搜索引擎从万维网上下载网页，是搜索引擎的重要组成。

[0003] 然而，网络爬虫的泛滥会导致网站信息的全面泄漏，因此部分网站有对网络爬虫进行限制的需求。在相关技术中，存在对网络爬虫和正常的业务请求识别困难以及识别准确度较低的问题。

## 发明内容

[0004] 基于此，有必要针对上述技术问题，提供一种访问请求的处理方法、装置、计算机设备、存储介质和计算机程序产品。

[0005] 第一方面，本公开提供了一种访问请求的处理方法。所述方法包括：

[0006] 接收客户端的实时访问请求，并根据所述实时访问请求的头部信息获取风控关键字；

[0007] 基于所述风控关键字在风险数据库中查询所述风控关键字对应的风险标注结果；所述风险数据库用于存储风控关键字和风险标注结果的对应关系；

[0008] 在所述风险数据库中查询到所述风控关键字对应的风险标注结果的情况下，将所述风险标注结果写入所述实时访问请求的头部信息中，得到标识访问请求；

[0009] 将所述标识访问请求发送至所述标识访问请求对应的应用终端，所述标识访问请求用于指示所述应用终端在根据所述风险标注结果确定所述标识访问请求触发风控规则时，对所述标识访问请求执行相应的风控处理动作。

[0010] 在其中一个实施例中，所述方法还包括：

[0011] 在所述风险数据库中未查询到所述风控关键字对应的风险标注结果的情况下，将所述实时访问请求推送至消息队列；

[0012] 从所述消息队列中读取所述实时访问请求，按照预设的风险规则匹配所述实时访问请求的风控关键字，获得所述实时访问请求对应的风险标注结果；

[0013] 将所述风险标注结果写入所述实时访问请求的头部信息中，得到所述标识访问请求；

[0014] 将所述标识访问请求的风控关键字与所述风险标注结果存储至所述风险数据库。

[0015] 在其中一个实施例中，所述方法还包括：

[0016] 按照设定的时间间隔获取历史访问请求，并获取所述历史访问请求的风控关键

字；

[0017] 按照预设的风险规则匹配所述历史访问请求的风控关键字，获得所述历史访问请求对应的风险标注结果；

[0018] 将所述历史访问请求的风控关键字与所述历史访问请求对应的风险标注结果存储至所述风险数据库。

[0019] 在其中一个实施例中，所述应用终端在根据所述风险标注结果确定所述标识访问请求触发风控规则时，对所述标识访问请求执行相应的风控处理动作包括：

[0020] 所述应用终端根据所述标识访问请求的风控关键字在风控规则数据库中查询所述风控关键字对应的风控规则；所述风控规则数据库用于存储风控关键字和风控规则的对应关系；

[0021] 响应于在风控规则数据库中查询到所述风控关键字对应的风控规则，所述应用终端根据所述标识访问请求对应的风控规则向所述客户端返回风控指令，所述风控指令用于指示所述客户端执行所述风控处理动作。

[0022] 在其中一个实施例中，所述风控处理动作包括动态验证码验证动作、滑动验证码验证动作、封禁提示动作或强制登录动作中的一种或多种。

[0023] 在其中一个实施例中，所述标识访问请求还用于指示所述应用终端在根据所述风险标注结果确定所述标识访问请求未触发所述风控规则时，向所述客户端返回所述标识访问请求的请求结果。

[0024] 在其中一个实施例中，所述应用终端在根据所述风险标注结果确定所述标识访问请求未触发所述风控规则时，向所述客户端返回所述标识访问请求的请求结果包括：

[0025] 所述应用终端根据所述标识访问请求的风控关键字在风控规则数据库中查询所述风控关键字对应的风控规则；所述风控规则数据库用于存储风控关键字和风控规则的对应关系；

[0026] 响应于在风控规则数据库中未查询到所述风控关键字对应的风控规则，所述应用终端根据所述标识访问请求向所述客户端返回请求结果。

[0027] 第二方面，本公开还提供了一种访问请求的处理装置。所述装置包括：

[0028] 实时访问请求模块，用于接收客户端的实时访问请求，并根据所述实时访问请求的头部信息获取风控关键字；

[0029] 风险查询模块，用于基于所述风控关键字在风险数据库中查询所述风控关键字对应的风险标注结果；所述风险数据库用于存储风控关键字和风险标注结果的对应关系；

[0030] 标识访问请求模块，用于在所述风险数据库中查询到所述风控关键字对应的风险标注结果的情况下，将所述风险标注结果写入所述实时访问请求的头部信息中，得到标识访问请求；

[0031] 请求处理模块，用于将所述标识访问请求发送至所述标识访问请求对应的应用终端，所述标识访问请求用于指示所述应用终端在根据所述风险标注结果确定所述标识访问请求触发风控规则时，对所述标识访问请求执行相应的风控处理动作。

[0032] 在其中一个实施例中，所述装置还包括：

[0033] 消息队列模块，用于在所述风险数据库中未查询到所述风控关键字对应的风险标注结果的情况下，将所述实时访问请求推送至消息队列；

[0034] 第一风险规则匹配模块，用于从所述消息队列中读取所述实时访问请求，按照预设的风险规则匹配所述实时访问请求的风控关键字，获得所述实时访问请求对应的风险标注结果；

[0035] 第二标注结果写入模块，用于将所述风险标注结果写入所述实时访问请求的头部信息中，得到所述标识访问请求；

[0036] 第一标注结果存储模块，用于将所述标识访问请求的风控关键字与所述风险标注结果存储至所述风险数据库。

[0037] 在其中一个实施例中，所述装置还包括：

[0038] 历史访问请求模块，用于按照设定的时间间隔获取历史访问请求，并获取所述历史访问请求的风控关键字；

[0039] 第二风险规则匹配模块，用于按照预设的风险规则匹配所述历史访问请求的风控关键字，获得所述历史访问请求对应的风险标注结果；

[0040] 第二标注结果存储模块，用于将所述历史访问请求的风控关键字与所述历史访问请求对应的风险标注结果存储至所述风险数据库。

[0041] 在其中一个实施例中，所述请求处理模块包括：

[0042] 风控规则查询单元，用于指示所述应用终端根据所述标识访问请求的风控关键字在风控规则数据库中查询所述风控关键字对应的风控规则；所述风控规则数据库用于存储风控关键字和风控规则的对应关系；

[0043] 风控指令返回单元，用于指示所述应用终端响应于在风控规则数据库中查询到所述风控关键字对应的风控规则，根据所述标识访问请求对应的风控规则向所述客户端返回风控指令，所述风控指令用于指示所述客户端执行所述风控处理动作。

[0044] 在其中一个实施例中，所述风控处理动作包括动态验证码验证动作、滑动验证码验证动作、封禁提示动作或强制登录动作中的一种或多种。

[0045] 在其中一个实施例中，所述标识访问请求还用于指示所述应用终端在根据所述风险标注结果确定所述标识访问请求未触发所述风控规则时，向所述客户端返回所述标识访问请求的请求结果。

[0046] 在其中一个实施例中，所述请求处理模块还包括：

[0047] 请求结果返回单元，用于指示所述应用终端响应于在风控规则数据库中未查询到所述风控关键字对应的风控规则，根据所述标识访问请求向所述客户端返回请求结果。

[0048] 第三方面，本公开还提供了一种计算机设备。所述计算机设备包括存储器和处理器，所述存储器存储有计算机程序，所述处理器执行所述计算机程序时实现上述访问请求的处理方法的步骤。

[0049] 第四方面，本公开还提供了一种计算机可读存储介质。所述计算机可读存储介质，其上存储有计算机程序，所述计算机程序被处理器执行时实现上述访问请求的处理方法的步骤。

[0050] 第五方面，本公开还提供了一种计算机程序产品。所述计算机程序产品，包括计算机程序，该计算机程序被处理器执行时实现上述访问请求的处理方法的步骤。

[0051] 上述访问请求的处理方法、装置、计算机设备、存储介质和计算机程序产品，至少包括以下有益效果：

[0052] 本公开通过对接收到的初始的实时访问请求进行风控关键字提取，并查询风控关键字的风险标注结果，将风险标注结果写入初始的实时访问请求中得到携带有风险标注结果的标识访问请求，将标识访问请求转发至应用终端，进而指示应用终端在根据风险标注结果确定标识访问请求触发风控规则时，对标识访问请求执行相应的风控处理动作，使得应用终端在响应访问请求之前对访问请求进行风险判断，便于区分客户端正常的业务请求和需要限制的网络爬虫，对爬虫识别和响应业务请求做一定的解耦处理，便于对爬虫识别的风险数据库、风险规则和风控规则进行灵活配置以适应不同的业务场景；同时提高了爬虫识别和业务请求的识别准确率，减少因识别不准对业务请求的负面影响，且有效地降低了信息泄露的风险。

## 附图说明

[0053] 为了更清楚地说明本公开实施例或传统技术中的技术方案，下面将对实施例或传统技术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公开的一些实施例，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他的附图。

[0054] 图1为一个实施例中访问请求的处理方法的应用环境图；

[0055] 图2为一个实施例中访问请求的处理方法的流程示意图；

[0056] 图3为另一个实施例中访问请求的处理方法的流程示意图；

[0057] 图4为又一个实施例中访问请求的处理方法的流程示意图；

[0058] 图5为一个实施例中向客户端返回风控指令的流程示意图；

[0059] 图6为一个实施例中向客户端返回请求结果的流程示意图；

[0060] 图7为一个实施例中访问请求的处理方法的服务架构示意图；

[0061] 图8为一个实施例中访问请求的处理装置的结构框图；

[0062] 图9为另一个实施例中访问请求的处理装置的结构框图；

[0063] 图10为又一个实施例中访问请求的处理装置的结构框图；

[0064] 图11为一个实施例中请求处理模块的结构框图；

[0065] 图12为另一个实施例中请求处理模块的结构框图；

[0066] 图13为一个实施例中计算机设备的内部结构框图。

## 具体实施方式

[0067] 为了使本申请的目的、技术方案及优点更加清楚明白，以下结合附图及实施例，对本申请进行进一步详细说明。应当理解，此处描述的具体实施例仅仅用以解释本申请，并不用于限定本申请。

[0068] 除非另有定义，本文所使用的所有的技术和科学术语与属于本公开的技术领域的技术人员通常理解的含义相同。本文中在本公开的说明书中所使用的术语只是为了描述具体的实施例的目的，不是旨在于限制本公开。

[0069] 需要说明的是，本公开的说明书和权利要求书及上述附图中的术语“第一”、“第二”等是用于区别类似的对象，而不必用于描述特定的顺序或先后次序。应该理解这样使用的数据在适当情况下可以互换，以便这里描述的本公开的实施例能够以除了在这里图示或

描述的那些以外的顺序实施。以下示例性实施例中所描述的实施方式并不代表与本公开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、本公开的一些方面相一致的装置和方法的例子。术语“包括”、“包含”或者其任何其它变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、产品或者设备不仅包括那些要素，而且还包括没有明确列出的其它要素，或者是还包括为这种过程、方法、产品或者设备所固有的要素。在没有更多限制的情况下，并不排除在包括所述要素的过程、方法、产品或者设备中还存在另外的相同或等同要素。例如若使用到第一，第二等词语用来表示名称，而并不表示任何特定的顺序。

[0070] 在此使用时，单数形式的“一”、“一个”和“所述/该”也可以包括复数形式，除非上下文清楚指出另外的方式。还应当理解的是，术语“包括/包含”或“具有”等指定所陈述的特征、整体、步骤、操作、组件、部分或它们的组合的存在，但是不排除存在或添加一个或更多个其他特征、整体、步骤、操作、组件、部分或它们的组合的可能性。同时，在本说明书中，术语“和/或”包括相关所列项目的任何及所有组合。

[0071] 本公开实施例提供的访问请求的处理方法，可以应用于如图1所示的应用环境中。其中，客户端102通过网络与服务器104进行通信。数据存储系统可以存储服务器104需要处理的数据。数据存储系统可以集成在服务器104上，也可以放在云上或其他网络服务器上。客户端102可以向服务器104发送访问请求，服务器104可以接收客户端102的访问请求并分析该访问请求的风险，在无风险情况下返回客户端102请求结果；在有风险情况下返回客户端102访问请求的处理动作。

[0072] 其中，服务器104包括网关106和应用终端108，网关106用于接收客户端102发送的访问请求，并对该访问请求的风险进行分析，并将风险结果写入访问请求后转发至应用终端108。应用终端108用于根据访问请求携带的风险结果返回请求结果或者风控处理动作。应用终端108可以是业务系统处理业务的应用端。

[0073] 客户端102可以但不限于是各种个人计算机、笔记本电脑、智能手机、平板电脑、物联网设备和便携式可穿戴设备，物联网设备可为智能音箱、智能电视、智能空调、智能车载设备等。便携式可穿戴设备可为智能手表、智能手环、头戴设备等。服务器104可以用独立的服务器或者是多个服务器组成的服务器集群来实现。

[0074] 在本公开的一些实施例中，如图2所示，提供了一种访问请求的处理方法，以该方法应用于图1中的网关为例进行说明，包括以下步骤：

[0075] 步骤210，接收客户端的实时访问请求，并根据所述实时访问请求的头部信息获取风控关键字。

[0076] 示例性地，网关可以接收客户端的实时访问请求，实时访问请求可以采用http协议(Hypertext Transfer Protocol，超文本传输协议)进入网关。网关程序可以解析实时访问请求，可以从实时访问请求的头部信息中提取风控关键字。其中，实时访问请求的头部信息可以是指http消息的消息头，消息头通常用于描述http消息正在获取的资源、服务器或者客户端的行为，定义了http事务中的具体操作参数等。头部信息的风控关键字可以包括实时访问请求的IP信息(Internet Protocol，网际互连协议)和令牌。令牌通常是指在计算机身份认证中的(临时)令牌，具有标记的意思，一般作为邀请、登录系统使用。

[0077] 步骤220，基于所述风控关键字在风险数据库中查询所述风控关键字对应的风险

标注结果;所述风险数据库用于存储风控关键字和风险标注结果的对应关系。

[0078] 示例性地,网关程序在提取出实时访问请求头部信息的风控关键字后,基于该风控关键字在风险数据库中查询风控关键字对应的风险标注结果。其中,风险数据库中存储有风控关键字和风险标注结果的对应关系,例如以键值对的形式存储风控关键字和其对应的风险标注结果。

[0079] 步骤230,在所述风险数据库中查询到所述风控关键字对应的风险标注结果的情况下,将所述风险标注结果写入所述实时访问请求的头部信息中,得到标识访问请求。

[0080] 示例性地,网关程序基于风控关键字在风险数据库中查询风险标注结果时,通常会有查询到风险标注结果和未查询到风险标注结果两种情况。在查询到风控关键字对应的风险标注结果的情况下,网关程序将查询到的风险标注结果写入实时访问请求的头部信息中,得到携带有风险标注结果的标识访问请求。风险标注结果可以包括表征实时访问请求是否具有风险的标注或者表征实时访问请求的风险等级/种类的标注等。例如,风险标注结果可以用数字或字母表示,不同的数字/字母可以用于表征无风险、低风险、中风险、高风险等。

[0081] 步骤240,将所述标识访问请求发送至所述标识访问请求对应的应用终端,所述标识访问请求用于指示所述应用终端在根据所述风险标注结果确定所述标识访问请求触发风控规则时,对所述标识访问请求执行相应的风控处理动作。

[0082] 示例性地,网关程序在得到标识访问请求后,可以将标识访问请求转发至服务器中的标识访问请求对应的应用终端。其中,标识访问请求可以用于指示应用终端根据风险标注结果对标识访问请求做出处理。其中,在应用终端根据风险标注结果确定所述标识访问请求触发风控规则时,标识访问请求用于指示应用终端对标识访问请求执行相应的风控处理动作。

[0083] 上述访问请求的处理方法中,通过对接收到的初始的实时访问请求进行风控关键字提取,并查询风控关键字的风险标注结果,将风险标注结果写入初始的实时访问请求中得到携带有风险标注结果的标识访问请求,将标识访问请求转发至应用终端,进而指示应用终端在根据风险标注结果确定标识访问请求触发风控规则时,对标识访问请求执行相应的风控处理动作,使得应用终端在响应访问请求之前对访问请求进行风险判断,便于区分客户端正常的业务请求和需要限制的网络爬虫,对爬虫识别和响应业务请求做一定的解耦处理,便于对爬虫识别的风险数据库、风险规则和风控规则进行灵活配置以适应不同的业务场景;同时提高了爬虫识别和业务请求的识别准确率,减少因识别不准对业务请求的负面影响,且有效地降低了信息泄露的风险。

[0084] 在本公开的一些实施例中,如图3所示,所述方法还包括:

[0085] 步骤232,在所述风险数据库中未查询到所述风控关键字对应的风险标注结果的情况下,将所述实时访问请求推送至消息队列。

[0086] 示例性地,在网关在风险数据库中未查询到风控关键字对应的风险标注结果的情况下,将实时访问请求推送至消息队列。消息队列可以是kafka队列,kafka通常是指一个由Apache软件基金会开发的开源流处理平台,Kafka是一种高吞吐量的分布式发布订阅消息系统,它可以处理消费者在网站中的所有动作流数据。

[0087] 步骤234,从所述消息队列中读取所述实时访问请求,按照预设的风险规则匹配所

述实时访问请求的风控关键字，获得所述实时访问请求对应的风险标注结果。

[0088] 示例性地，网关程序可以基于先进先出的机制，从消息队列中读取实时访问请求。根据实时访问请求的风控关键字，按照预设的风险规则进行匹配，可以得到该风控关键字对应的风险标注结果。例如根据实时访问请求的风控关键字，按照风险规则进行匹配后可以得到无风险、低风险、中风险或高风险等的风险标注结果。

[0089] 步骤236，将所述风险标注结果写入所述实时访问请求的头部信息中，得到标识访问请求。

[0090] 示例性地，网关程序可以将匹配得到的风险标注结果写入实时访问请求的头部信息中，得到携带有风险标注结果的标识访问请求。

[0091] 步骤238，将所述标识访问请求的风控关键字与所述风险标注结果存储至所述风险数据库。

[0092] 示例性地，网关程序还可以将匹配得到的风险标注结果和对应的风控关键字存入风险数据库，对风险数据库进行实时的扩充更新。

[0093] 本实施例在未查询到风控关键字对应的风险标注结果的情况下，通过消息队列对实时访问请求进行缓冲，避免实时访问请求的生产速度大于消费速度，并对实时访问请求的风控关键字进行匹配，得到实时访问请求的风险标注结果，进而得到标识访问请求，以及进行风险数据库的实时扩充更新。

[0094] 在本公开的一些实施例中，如图4所示，所述方法还包括：

[0095] 步骤250，按照设定的时间间隔获取历史访问请求，并获取所述历史访问请求的风控关键字。

[0096] 示例性地，网关程序不仅可以实时地对实时访问请求进行获取其风险标注结果的操作，还可以按照设定的时间间隔获取历史访问请求，并提取历史访问请求的风控关键字。

[0097] 步骤260，按照预设的风险规则匹配所述历史访问请求的风控关键字，获得所述历史访问请求对应的风险标注结果。

[0098] 示例性地，网关程序可以对历史访问请求的风控关键字按照预设的风险规则进行匹配，得到历史访问请求的风险标注结果。

[0099] 步骤270，将所述历史访问请求的风控关键字与所述历史访问请求对应的风险标注结果存储至所述风险数据库。

[0100] 示例性地，网关程序可以将历史访问请求的风控关键字和其对应的风险标注结果存储至风险数据库。可选地，在存入风险数据库之前，可以先查询风险数据库中是否包含历史访问请求的风控关键字和其对应的风险标注结果，若不存在，将历史访问请求的风控关键字和其对应的风险标注结果存储至风险数据库。

[0101] 本实施例通过获取历史访问请求的风险标注结果，对实时获取实时访问请求的风险标注结果做进一步的补充，起到查漏补缺的作用。

[0102] 在本公开的一些实施例中，如图5所示，应用终端对标识访问请求执行相应的风控处理动作包括：

[0103] 步骤510，所述应用终端根据所述标识访问请求的风控关键字在风控规则数据库中查询所述风控关键字对应的风控规则；所述风控规则数据库用于存储风控关键字和风控规则的对应关系。

[0104] 示例性地，应用终端可以根据标识访问请求的风控关键字在预设的风控规则数据库中查询风控关键字对应的风控规则，风控规则数据库中存储有风控关键字和风控规则的对应关系。例如可以根据风控关键字查询到对应的风控规则的标识。风控规则数据库可以以键值对的形式存储风控关键字和其对应的风控规则的标识。风控规则可以是用于规定风控关键字对应的风险标注结果是否存在风险或者风险标注结果存在的风险等级的规则。

[0105] 步骤520，响应于在风控规则数据库中查询到所述风控关键字对应的风控规则，所述应用终端根据所述标识访问请求对应的风控规则向所述客户端返回风控指令，所述风控指令用于指示所述客户端执行所述风控处理动作。

[0106] 示例性地，应用终端在风控规则数据库中查询到风控关键字对应的风控规则时，触发应用终端向客户端返回风控指令。风控指令用于指示客户端执行风控处理动作。

[0107] 本实施例的应用终端通过在风控规则数据库中查询风控关键字对应的风控规则，并在确定标识访问请求触发风控规则时，应用终端根据所述标识访问请求对应的风控规则向所述客户端返回风控指令，进而指示客户端执行风控处理动作，使得应用终端可以对存在风险的标识访问请求的客户端进行验证，降低信息泄露的风险。

[0108] 在本公开的一些实施例中，应用终端返回至客户端的风控指令中，可以包括对应的风控处理动作信息。风控处理动作可以包括动态验证码验证动作、滑动验证码验证动作、封禁提示动作或强制登录动作中的一种或多种。动态验证码验证动作可以是指通过显示界面显示动态验证码验证提示窗口。滑动验证码验证动作可以是指通过显示界面显示滑动验证码验证提示窗口。封禁提示动作可以是指通过显示界面显示封禁提示窗口。强制登录动作可以是指通过显示界面显示强制登录窗口。

[0109] 在本公开的一些实施例中，在步骤240中，标识访问请求还用于指示应用终端在根据风险标注结果确定标识访问请求未触发所述风控规则时，向客户端返回所述标识访问请求的请求结果。

[0110] 示例性地，网关程序可以将标识访问请求转发至服务器中的标识访问请求对应的应用终端。其中，在应用终端根据风险标注结果确定所述标识访问请求未触发风控规则时，标识访问请求用于指示应用终端向客户端返回标识访问请求的请求结果。

[0111] 本实施例通过对标识访问请求的风险标注结果进行解析，针对无风险的标识访问请求返回其请求结果，针对存在风险的标识访问请求返回风控指令，对客户端进行风控处理动作，有助于区分客户端的正常访问请求和网络爬虫，并返回相对应的处理。

[0112] 在本公开的一些实施例中，如图6所示，应用终端向所述客户端返回所述标识访问请求的请求结果包括：

[0113] 步骤610，所述应用终端根据所述标识访问请求的风控关键字在风控规则数据库中查询所述风控关键字对应的风控规则；所述风控规则数据库用于存储风控关键字和风控规则的对应关系。

[0114] 示例性地，应用终端可以根据标识访问请求的风控关键字在预设的风控规则数据库中查询风控关键字对应的风控规则，风控规则数据库中存储有风控关键字和风控规则的对应关系。例如可以根据风控关键字查询到对应的风控规则的标识。风控规则数据库可以以键值对的形式存储风控关键字和其对应的风控规则的标识。风控规则可以是用于规定风控关键字对应的风险标注结果是否存在风险或者风险标注结果存在的风险等级的规则。

[0115] 步骤620，响应于在风控规则数据库中未查询到所述风控关键字对应的风控规则，所述应用终端根据所述标识访问请求向所述客户端返回请求结果。

[0116] 示例性地，服务器的应用终端可以响应于在风控规则数据库中未查询到风控关键字对应的风控规则，即该标识访问请求未触发风控规则时，应用终端根据标识访问请求向所述客户端返回请求结果。

[0117] 本实施例通过对标注访问请求的风险标注结果进行解析，针对无风险的标注访问请求返回其请求结果，降低了泄露信息的风险。

[0118] 在本公开的一些实施例中，所述访问请求的处理方法通过如图7所示的服务架构实现。网关可以提供实时清洗程序和定时清洗程序。其中，网关可以实时接收客户端发送的实时访问请求，并根据实时访问请求的风控关键字在风险数据库中查询风控关键字对应的风险标注结果。查询结果可以包括以下两种情况：

[0119] (1)在风险数据库中查询到风控关键字对应的风险标注结果的情况下，网关可以将风险标注结果写入实时访问请求的头部信息形成标识访问请求，将携带有风险标注结果的标识访问请求转发至服务器的应用终端。

[0120] (2)在风险数据库中未查询到风控关键字对应的风险标注结果的情况下，网关可以向消息队列推送实时访问请求的请求日志。通过网关中的实时清洗程序消费请求日志，实时清洗程序可以根据实时访问请求的风控关键字按照预设的风险规则匹配得到风险标注结果，并写入实时访问请求的头部信息形成标识访问请求。实时清洗程序还可以将清洗后的携带有风险标注结果的标识访问请求推送到风险数据库，由网关再将标识访问请求转发至服务器的应用终端。其中，预设的风险规则可以从预设的风险规则数据库中获得。

[0121] 另外，网关还提供定时清洗程序，网关中的定时清洗程序可以按照设定的时间间隔从请求日志系统中获取历史访问请求，定时清洗程序可以根据历史访问请求的风控关键字按照预设的风险规则匹配得到风险标注结果，并将历史访问请求的风控关键字与历史访问请求对应的风险标注结果存储至风险数据库。

[0122] 应用终端可以提供针对风险标注结果的识别程序和风控验证程序。其中，识别程序可以对接收到的标识访问请求的风险标注结果进行识别，识别结果可以包括以下两种情况：

[0123] (1)识别程序判断标识访问请求是否触发了风控规则，判断得到结果为标识访问请求未触发风控规则，则向客户端返回标识访问请求的请求结果。

[0124] (2)识别程序判断标识访问请求触发了风控规则，则识别为标识访问请求存在风险，进而触发应用终端的风控验证程序。风控验证程序可以根据标识访问请求所触发的风险规则向客户端返回对应的风控指令。风控指令可以指示客户端执行风控处理动作，例如动态验证码验证动作、滑动验证码验证动作、封禁提示动作或强制登录动作中的一种或多种。例如，风险标注结果可以表征不同等级的风险，进而触发不同等级的风控规则，风控验证程序可以根据所触发的风控规则的等级发送该等级对应的风控指令，该风控指令可以指示对应等级的验证动作。

[0125] 本实施例通过网关和应用终端，将针对访问请求的清洗和响应访问请求进行了分离，同时网关通过实时清洗程序和定时清洗程序相配合实现对的访问请求的清洗过程，完成对访问请求的风险标注，便于应用终端根据访问请求的风险标注结果触发对应的处理动

作，大大提高了爬虫识别和业务请求的识别准确率，减少因识别不准对业务请求的负面影响，且有效地降低了信息泄露的风险。

[0126] 应该理解的是，虽然如上所述的各实施例所涉及的流程图中的各个步骤按照箭头的指示依次显示，但是这些步骤并不是必然按照箭头指示的顺序依次执行。除非本文中有明确的说明，这些步骤的执行并没有严格的顺序限制，这些步骤可以以其它的顺序执行。而且，如上所述的各实施例所涉及的流程图中的至少一部分步骤可以包括多个步骤或者多个阶段，这些步骤或者阶段并不必然是在同一时刻执行完成，而是可以在不同的时刻执行，这些步骤或者阶段的执行顺序也不必然是依次进行，而是可以与其它步骤或者其它步骤中的步骤或者阶段的至少一部分轮流或者交替地执行。

[0127] 基于同样的发明构思，本公开实施例还提供了一种用于实现上述所涉及的访问请求的处理方法的访问请求的处理装置。该装置所提供的解决问题的实现方案与上述方法中所记载的实现方案相似，故下面所提供的一个或多个访问请求的处理装置实施例中的具体限定可以参见上文中对于访问请求的处理方法的限定，在此不再赘述。

[0128] 在本公开的一些实施例中，如图8所示，提供了一种访问请求的处理装置。所述装置800包括：

[0129] 实时访问请求模块810，用于接收客户端的实时访问请求，并根据所述实时访问请求的头部信息获取风控关键字；

[0130] 风险查询模块820，用于基于所述风控关键字在风险数据库中查询所述风控关键字对应的风险标注结果；所述风险数据库用于存储风控关键字和风险标注结果的对应关系；

[0131] 第一标注结果写入模块830，用于在所述风险数据库中查询到所述风控关键字对应的风险标注结果的情况下，将所述风险标注结果写入所述实时访问请求的头部信息中，得到标识访问请求；

[0132] 请求处理模块840，用于将所述标识访问请求发送至所述标识访问请求对应的应用终端，所述标识访问请求用于指示所述应用终端在根据所述风险标注结果确定所述标识访问请求触发风控规则时，对所述标识访问请求执行相应的风控处理动作。

[0133] 在本公开的一些实施例中，如图9所示，所述装置800还包括：

[0134] 消息队列模块850，用于在所述风险数据库中未查询到所述风控关键字对应的风险标注结果的情况下，将所述实时访问请求推送至消息队列；

[0135] 第一风险规则匹配模块860，用于从所述消息队列中读取所述实时访问请求，按照预设的风险规则匹配所述实时访问请求的风控关键字，获得所述实时访问请求对应的风险标注结果；

[0136] 第二标注结果写入模块870，用于将所述风险标注结果写入所述实时访问请求的头部信息中，得到所述标识访问请求；

[0137] 第一标注结果存储模块880，用于将所述标识访问请求的风控关键字与所述风险标注结果存储至所述风险数据库。

[0138] 在本公开的一些实施例中，如图10所示，所述装置800还包括：

[0139] 历史访问请求模块890，用于按照设定的时间间隔获取历史访问请求，并获取所述历史访问请求的风控关键字；

[0140] 第二风险规则匹配模块892，用于按照预设的风险规则匹配所述历史访问请求的风控关键字，获得所述历史访问请求对应的风险标注结果；

[0141] 第二标注结果存储模块894，用于将所述历史访问请求的风控关键字与所述历史访问请求对应的风险标注结果存储至所述风险数据库。

[0142] 在本公开的一些实施例中，如图11所示，所述请求处理模块840包括：

[0143] 风控规则查询单元842，用于指示所述应用终端根据所述标识访问请求的风控关键字在风控规则数据库中查询所述风控关键字对应的风控规则；所述风控规则数据库用于存储风控关键字和风控规则的对应关系；

[0144] 风控指令返回单元844，用于指示所述应用终端响应于在风控规则数据库中查询到所述风控关键字对应的风控规则，根据所述标识访问请求对应的风控规则向所述客户端返回风控指令，所述风控指令用于指示所述客户端执行所述风控处理动作。

[0145] 在其中一个实施例中，所述风控处理动作包括动态验证码验证动作、滑动验证码验证动作、封禁提示动作或强制登录动作中的一种或多种。

[0146] 在本公开的一些实施例中，标识访问请求还用于指示所述应用终端在根据所述风险标注结果确定所述标识访问请求未触发所述风控规则时，向所述客户端返回所述标识访问请求的请求结果。

[0147] 在本公开的一些实施例中，如图12所示，所述请求处理模块840还包括：

[0148] 请求结果返回单元846，用于指示所述应用终端响应于在风控规则数据库中未查询到所述风控关键字对应的风控规则，根据所述标识访问请求向所述客户端返回请求结果。

[0149] 上述访问请求的处理装置中的各个模块可全部或部分通过软件、硬件及其组合来实现。上述各模块可以硬件形式内嵌于或独立于计算机设备中的处理器中，也可以以软件形式存储于计算机设备中的存储器中，以便于处理器调用执行以上各个模块对应的操作。需要说明的是，本公开实施例中对模块的划分是示意性的，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式。

[0150] 基于前述访问请求的处理方法的实施例描述，在本公开提供的另一个实施例中，提供了一种计算机设备，该计算机设备可以是服务器，其内部结构图可以如图13所示。该计算机设备包括处理器、存储器、输入/输出接口(Input/Output，简称I/O)和通信接口。其中，处理器、存储器和输入/输出接口通过系统总线连接，通信接口通过输入/输出接口连接到系统总线。其中，该计算机设备的处理器用于提供计算和控制能力。该计算机设备的存储器包括非易失性存储介质和内存储器。该非易失性存储介质存储有操作系统、计算机程序和数据库。该内存储器为非易失性存储介质中的操作系统和计算机程序的运行提供环境。该计算机设备的数据库用于存储数据。该计算机设备的输入/输出接口用于处理器与外部设备之间交换信息。该计算机设备的通信接口用于与外部的终端通过网络连接通信。该计算机程序被处理器执行时以实现一种访问请求的处理方法。

[0151] 本领域技术人员可以理解，图13中示出的结构，仅仅是与本申请方案相关的部分结构的框图，并不构成对本申请方案所应用于其上的计算机设备的限定，具体的计算机设备可以包括比图中所示更多或更少的部件，或者组合某些部件，或者具有不同的部件布置。

[0152] 基于前述访问请求的处理方法的实施例描述，在本公开提供的另一个实施例中，

提供了一种计算机可读存储介质，其上存储有计算机程序，计算机程序被处理器执行时实现上述各方法实施例中的步骤。

[0153] 基于前述访问请求的处理方法的实施例描述，在本公开提供的另一个实施例中，提供了一种计算机程序产品，包括计算机程序，该计算机程序被处理器执行时实现上述各方法实施例中的步骤。

[0154] 本领域普通技术人员可以理解实现上述实施例方法中的全部或部分流程，是可以通过计算机程序来指令相关的硬件来完成，所述的计算机程序可存储于一非易失性计算机可读取存储介质中，该计算机程序在执行时，可包括如上述各方法的实施例的流程。其中，本申请所提供的各实施例中所使用的对存储器、数据库或其它介质的任何引用，均可包括非易失性和易失性存储器中的至少一种。非易失性存储器可包括只读存储器(Read-Only Memory，ROM)、磁带、软盘、闪存、光存储器、高密度嵌入式非易失性存储器、阻变存储器(ReRAM)、磁变存储器(Magnetoresistive Random Access Memory，MRAM)、铁电存储器(Ferroelectric Random Access Memory，FRAM)、相变存储器(Phase Change Memory，PCM)、石墨烯存储器等。易失性存储器可包括随机存取存储器(Random Access Memory，RAM)或外部高速缓冲存储器等。作为说明而非局限，RAM可以是多种形式，比如静态随机存取存储器(Static Random Access Memory，SRAM)或动态随机存取存储器(Dynamic Random Access Memory，DRAM)等。本申请所提供的各实施例中所涉及的数据库可包括关系型数据库和非关系型数据库中至少一种。非关系型数据库可包括基于区块链的分布式数据库等，不限于此。本申请所提供的各实施例中所涉及的处理器可为通用处理器、中央处理器、图形处理器、数字信号处理器、可编程逻辑器、基于量子计算的数据处理逻辑器等，不限于此。

[0155] 在本说明书的描述中，参考术语“有些实施例”、“其他实施例”、“理想实施例”等的描述意指结合该实施例或示例描述的具体特征、结构、材料或者特征包含于本发明的至少一个实施例或示例中。在本说明书中，对上述术语的示意性描述不一定指的是相同的实施例或示例。

[0156] 可以理解的是，本说明书中上述方法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它实施例的不同之处。相关之处参见其他方法实施例的描述说明即可。

[0157] 上所述实施例的各技术特征可以进行任意的组合，为使描述简洁，未对上述实施例各个技术特征所有可能的组合都进行描述，然而，只要这些技术特征的组合不存在矛盾，都应当认为是本说明书记载的范围。

[0158] 以上所述实施例仅表达了本公开的几种实施方式，其描述较为具体和详细，但并不能因此而理解为对申请专利范围的限制。应当指出的是，对于本领域的普通技术人员来说，在不脱离本公开构思的前提下，还可以做出若干变形和改进，这些都属于本公开的保护范围。因此，本公开专利的保护范围应以所附权利要求为准。

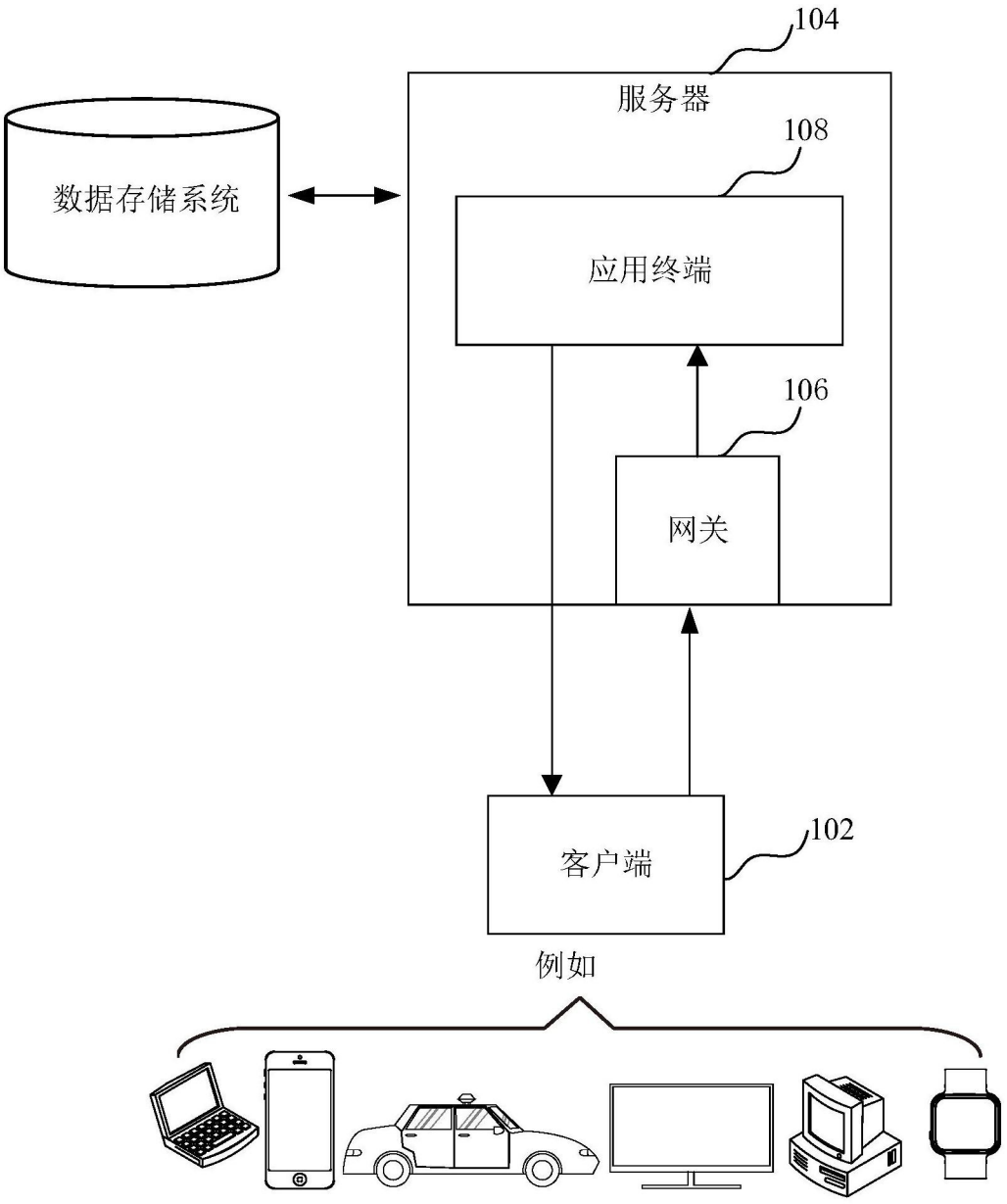



图1

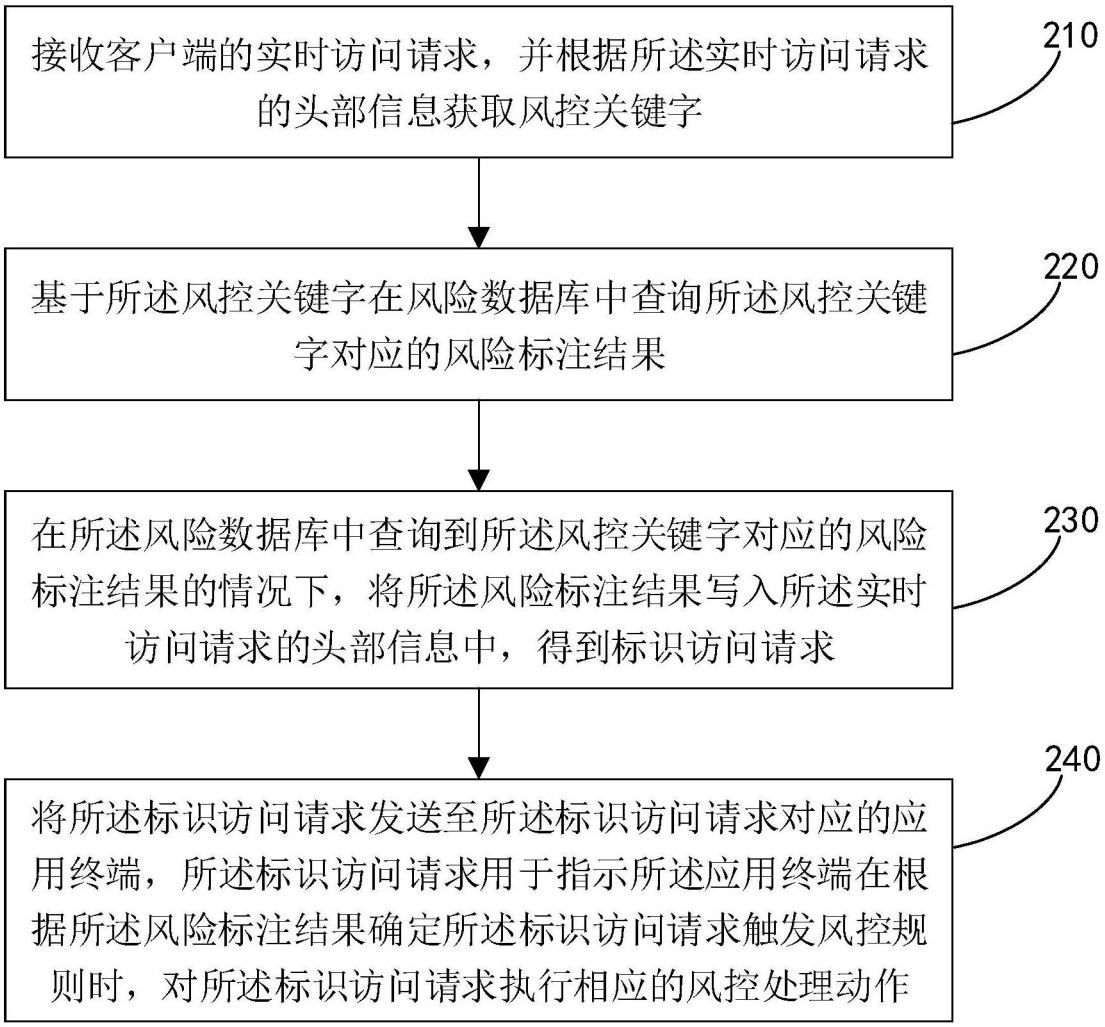

接收客户端的实时访问请求，并根据所述实时访问请求的头部信息获取风控关键字
210
基于所述风控关键字在风险数据库中查询所述风控关键字对应的风险标注结果
220
在所述风险数据库中查询到所述风控关键字对应的风险标注结果的情况下，将所述风险标注结果写入所述实时访问请求的头部信息中，得到标识访问请求
230
将所述标识访问请求发送至所述标识访问请求对应的应用终端，所述标识访问请求用于指示所述应用终端在根据所述风险标注结果确定所述标识访问请求触发风控规则时，对所述标识访问请求执行相应的风控处理动作
240

图2

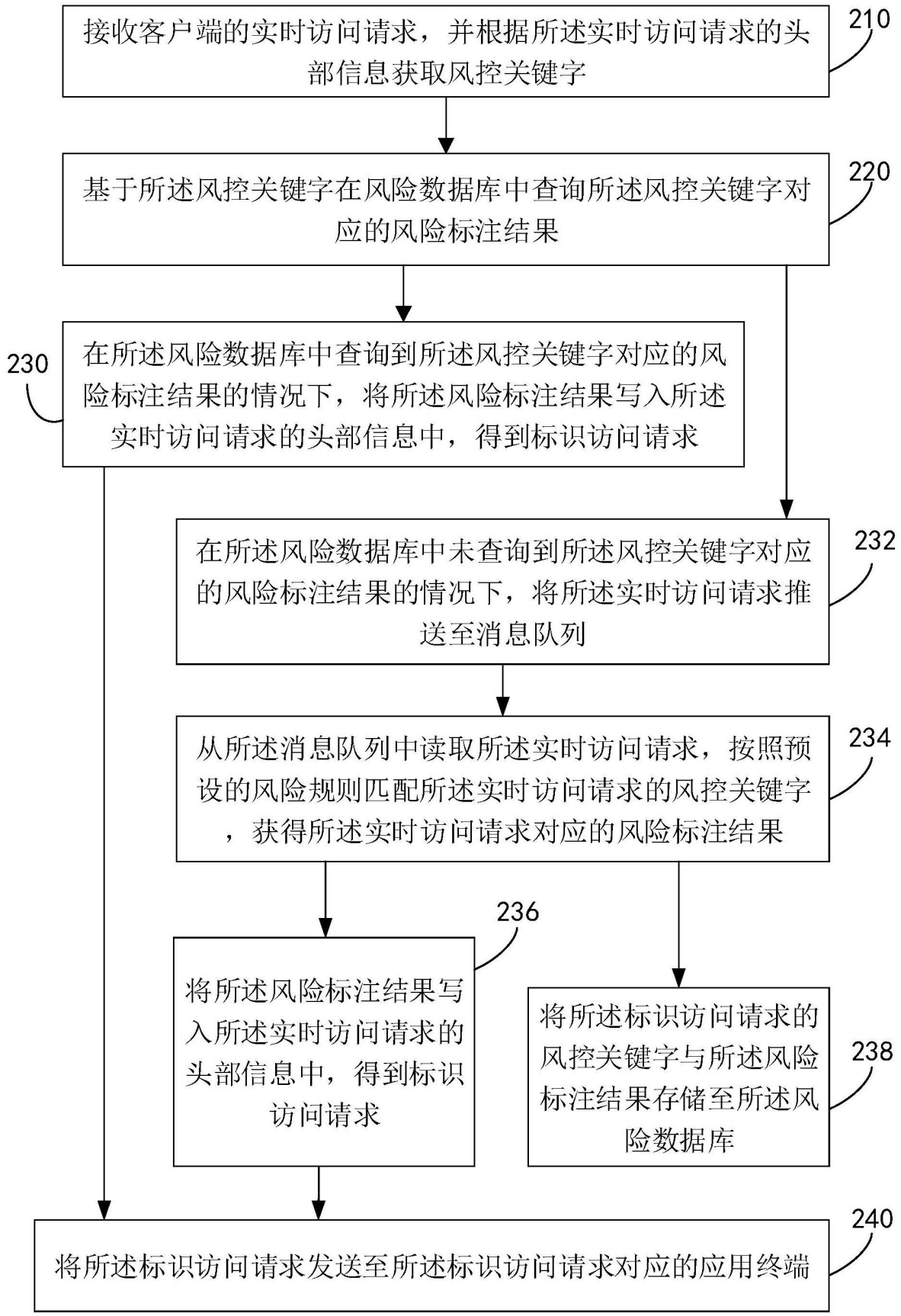

接收客户端的实时访问请求，并根据所述实时访问请求的头部信息获取风控关键字
210
基于所述风控关键字在风险数据库中查询所述风控关键字对应的风险标注结果
220
230
在所述风险数据库中查询到所述风控关键字对应的风险标注结果的情况下，将所述风险标注结果写入所述实时访问请求的头部信息中，得到标识访问请求
在所述风险数据库中未查询到所述风控关键字对应的风险标注结果的情况下，将所述实时访问请求推送至消息队列
232
从所述消息队列中读取所述实时访问请求，按照预设的风险规则匹配所述实时访问请求的风控关键字，获得所述实时访问请求对应的风险标注结果
234
236
将所述风险标注结果写入所述实时访问请求的头部信息中，得到标识访问请求
将所述标识访问请求的风控关键字与所述风险标注结果存储至所述风险数据库
238
240
将所述标识访问请求发送至所述标识访问请求对应的应用终端

图3

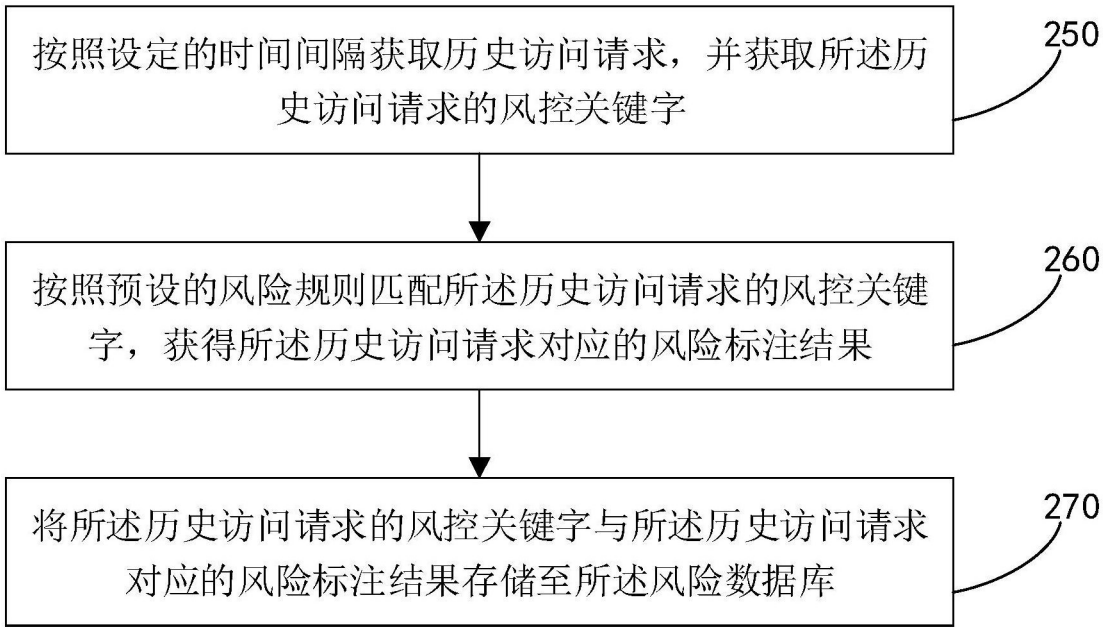

按照设定的时间间隔获取历史访问请求，并获取所述历史访问请求的风控关键字
250
按照预设的风险规则匹配所述历史访问请求的风控关键字，获得所述历史访问请求对应的风险标注结果
260
将所述历史访问请求的风控关键字与所述历史访问请求对应的风险标注结果存储至所述风险数据库
270

图4

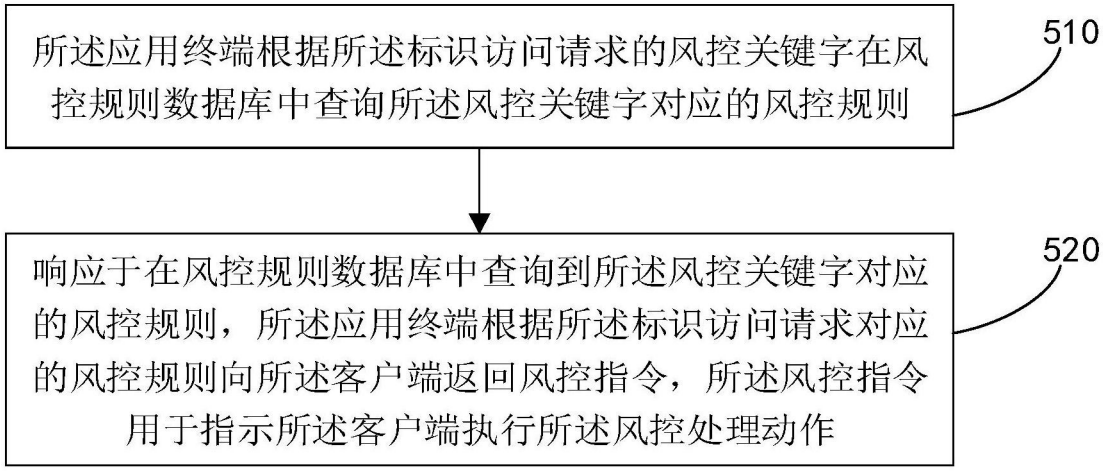

所述应用终端根据所述标识访问请求的风控关键字在风控规则数据库中查询所述风控关键字对应的风控规则
510
响应于在风控规则数据库中查询到所述风控关键字对应的风控规则，所述应用终端根据所述标识访问请求对应的风控规则向所述客户端返回风控指令，所述风控指令用于指示所述客户端执行所述风控处理动作
520

图5

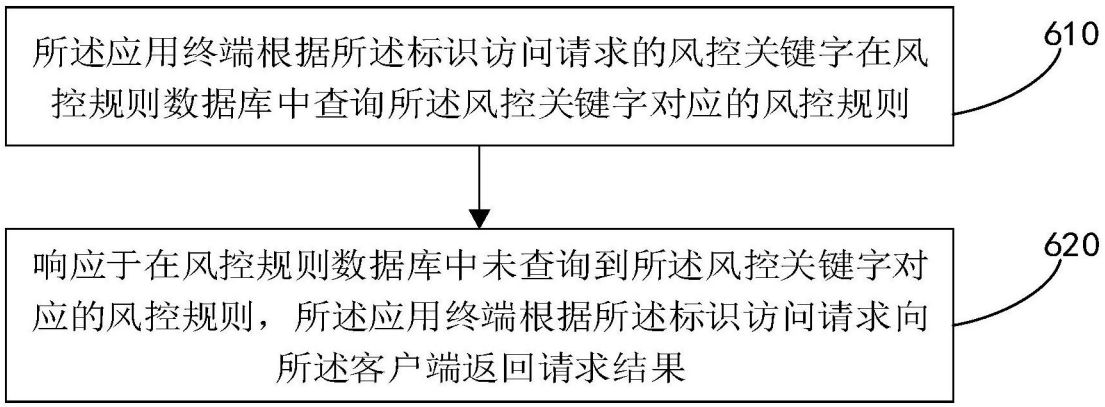

所述应用终端根据所述标识访问请求的风控关键字在风控规则数据库中查询所述风控关键字对应的风控规则
610
响应于在风控规则数据库中未查询到所述风控关键字对应的风控规则，所述应用终端根据所述标识访问请求向所述客户端返回请求结果
620

图6

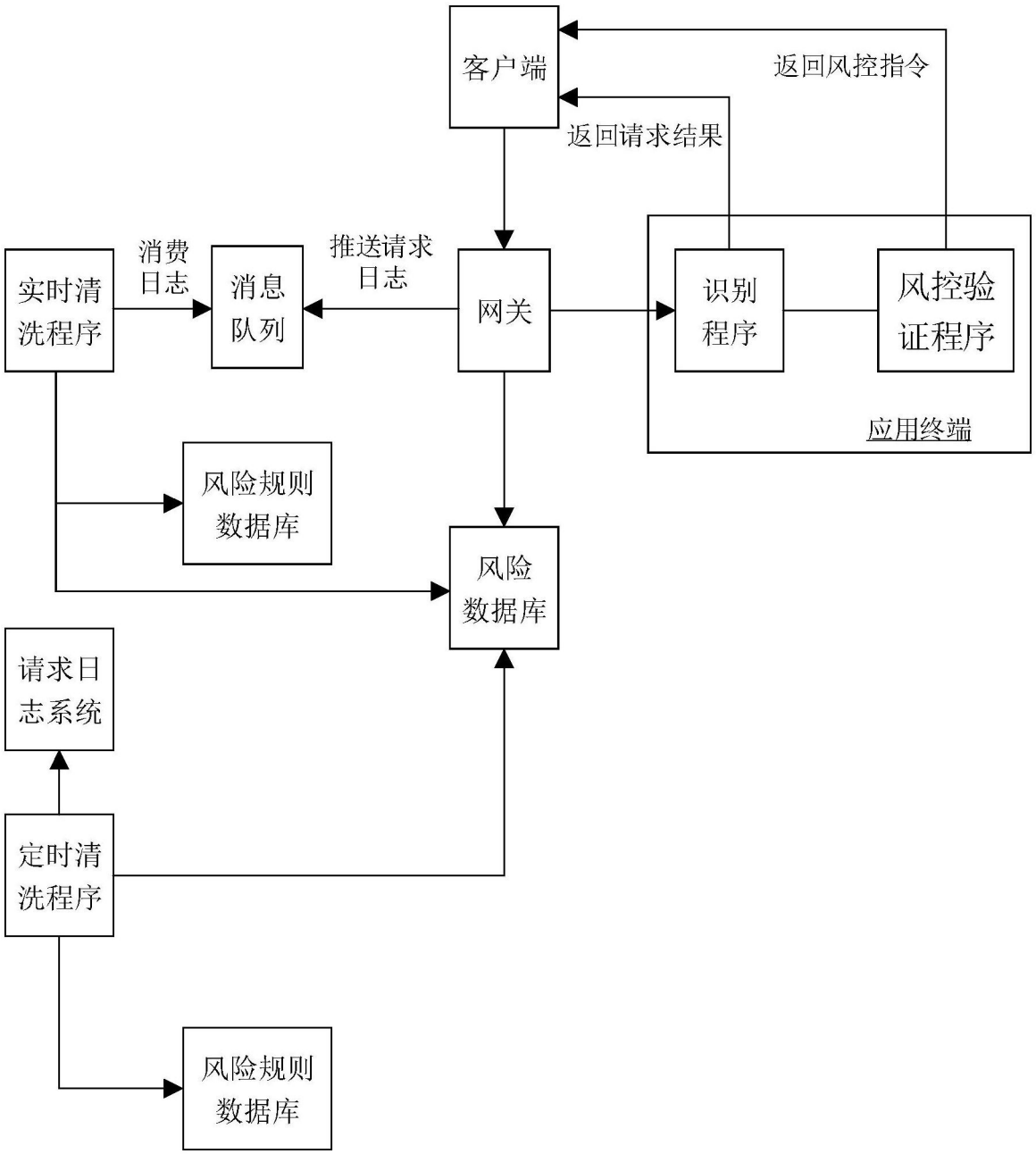

客户端
返回风控指令
返回请求结果
消费
日志
推送请求
日志
实时清
洗程序
消息
队列
网关
识别
程序
风控验
证程序
应用终端
风险规则
数据库
风险
数据库
请求日
志系统
定时清
洗程序
风险规则
数据库

图7

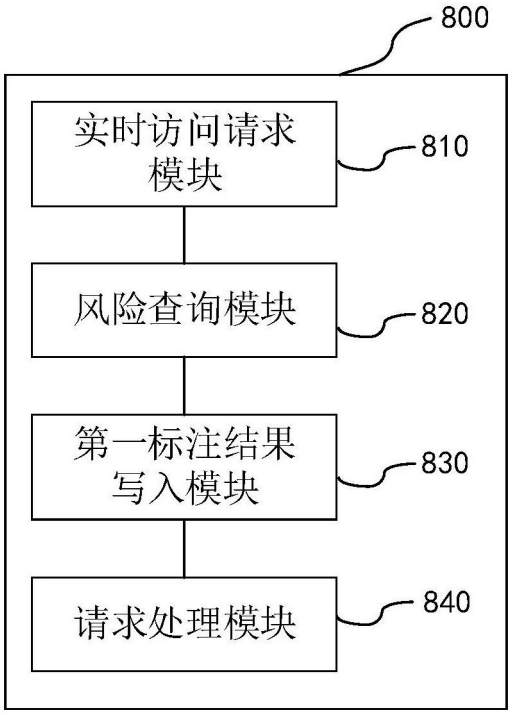

800
实时访问请求模块
810
风险查询模块
820
第一标注结果写入模块
830
请求处理模块
840

图8

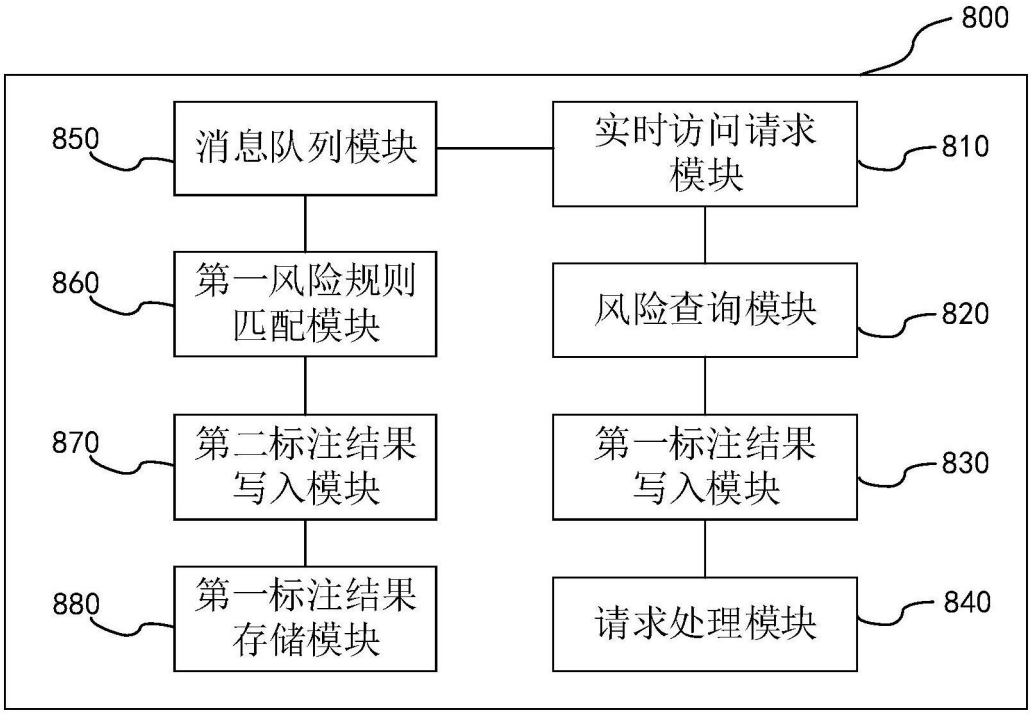

800
850
消息队列模块
实时访问请求模块
810
860
第一风险规则匹配模块
风险查询模块
820
870
第二标注结果写入模块
第一标注结果写入模块
830
880
第一标注结果存储模块
请求处理模块
840

图9

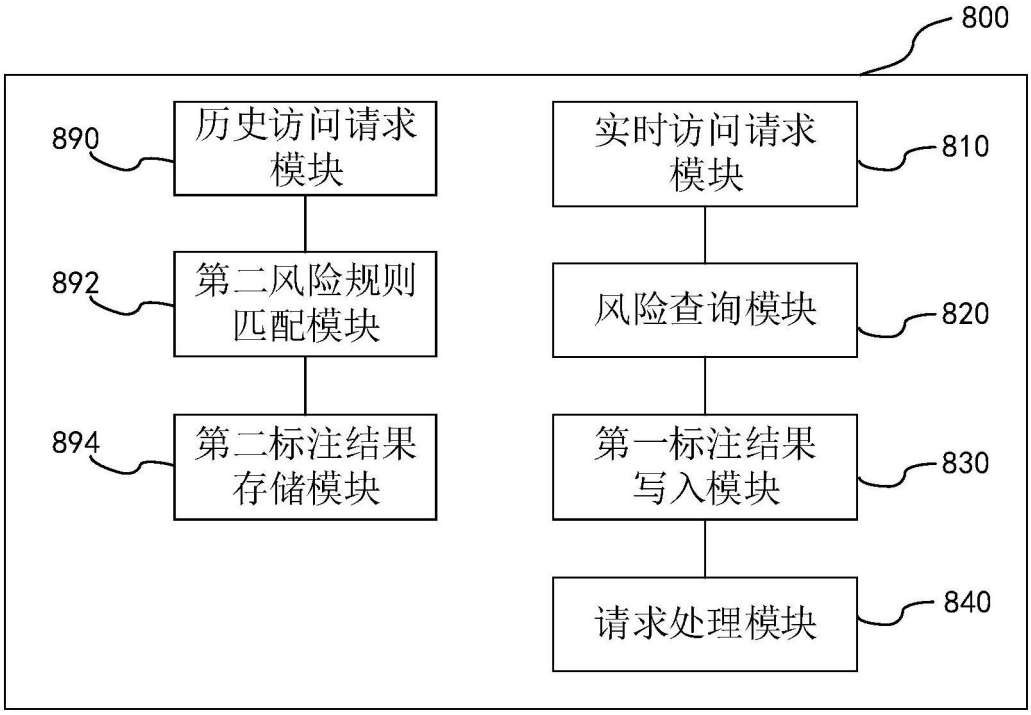

800
890
历史访问请求模块
892
第二风险规则匹配模块
894
第二标注结果存储模块
实时访问请求模块
810
风险查询模块
820
第一标注结果写入模块
830
请求处理模块
840

图10

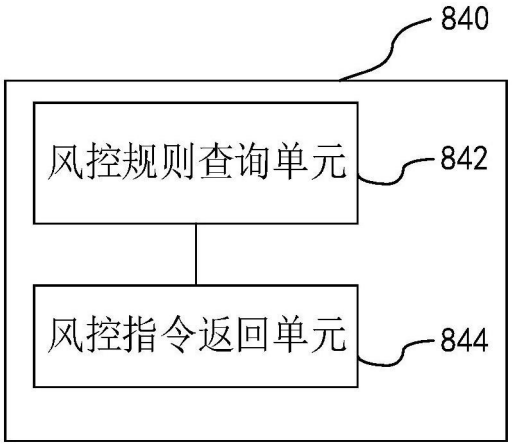

840
风控规则查询单元
842
风控指令返回单元
844

图11

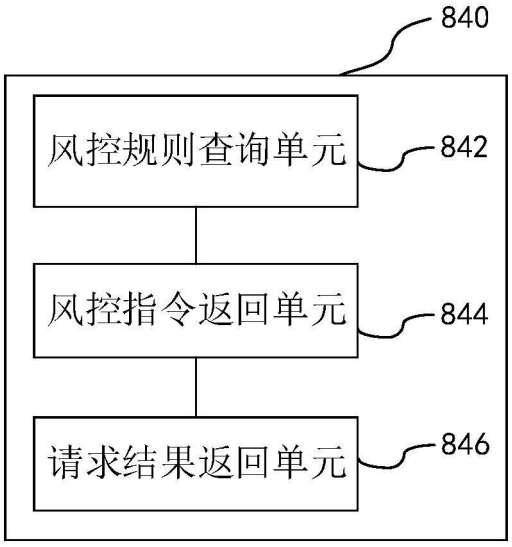

840
风控规则查询单元
842
风控指令返回单元
844
请求结果返回单元
846

图12

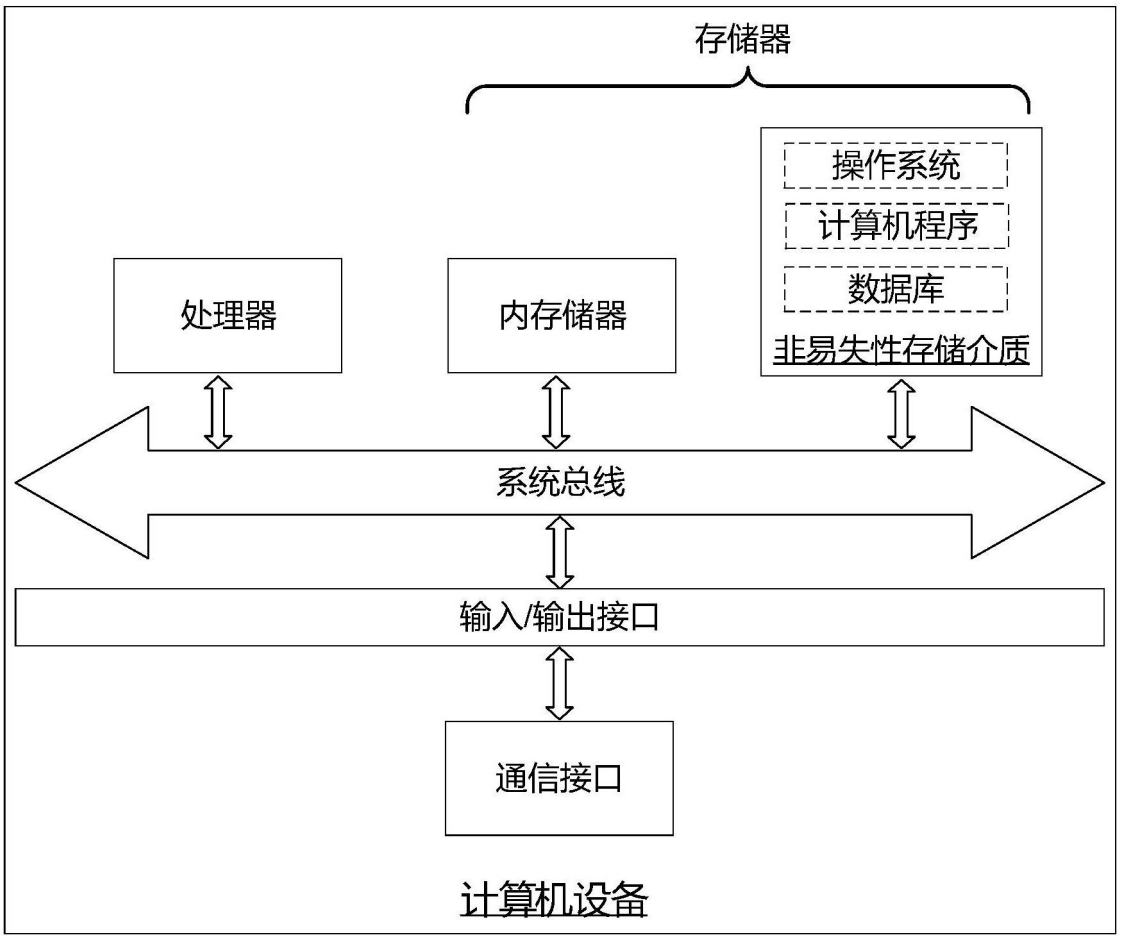

存储器
操作系统
计算机程序
数据库
非易失性存储介质
处理器
内存储器
系统总线
输入/输出接口
通信接口
计算机设备

图13