(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 111431908 A
(43)申请公布日 2020.07.17

(21)申请号 202010227882.0

(22)申请日 2020.03.26

(71)申请人 深圳壹账通智能科技有限公司
地址 518000 广东省深圳市前海深港合作区前湾一路1号A栋201室(入驻深圳市前海商务秘书有限公司)

(72)发明人 余自雷 王振华

(74)专利代理机构 广州三环专利商标代理有限公司 44202
代理人 熊永强 彭程

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 9/32(2006.01)

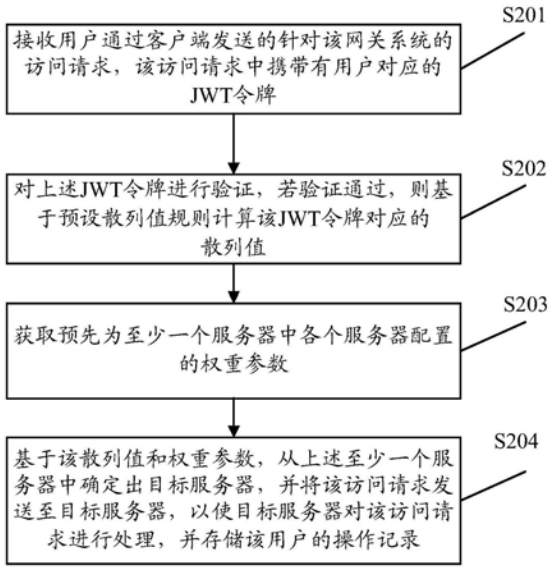
权利要求书2页 说明书11页 附图4页

(54)发明名称

一种访问处理方法、装置及可读存储介质

(57)摘要

本发明实施例公开了一种访问处理方法、装置及可读存储介质,该访问处理方法应用于网关系统对应的管理服务器,该管理服务器用于管理至少一个服务器,该访问处理方法包括:接收用户通过客户端发送的针对网关系统的访问请求,该访问请求携带有用户对应的JWT令牌;对JWT令牌进行验证,若验证通过,则基于预设散列值规则计算JWT令牌对应的散列值;获取预先为各个服务器配置的权重参数;基于散列值和权重参数,从至少一个服务器中确定出目标服务器,并将访问请求发送至目标服务器。采用这样的访问处理方法,可以使同一用户的访问请求被同一目标服务器处理,同一个用户的操作记录被同一个目标服务器存储,有利于提高同一用户操作记录的连续性。



CN 111431908 A

1.一种访问处理方法,其特征在于,所述方法应用于网关系统对应的管理服务器,所述管理服务器用于管理至少一个服务器,所述方法包括:

接收用户通过客户端发送的针对所述网关系统的访问请求,所述访问请求携带有所述用户对应的JWT令牌;

对所述JWT令牌进行验证,若验证通过,则基于预设散列值规则计算所述JWT令牌对应的散列值;

获取预先为所述至少一个服务器中各个服务器配置的权重参数;

基于所述散列值和所述权重参数,从所述至少一个服务器中确定出目标服务器,并将所述访问请求发送至所述目标服务器,以使所述目标服务器对所述访问请求进行处理,并存储所述用户的操作记录。

2.根据权利要求1所述方法,其特征在于,所述接收用户通过客户端发送的针对所述网关系统的访问请求之前,所述方法还包括:

接收用户通过客户端提交的用户账号信息和用户密钥,并对所述用户账号信息和所述用户密钥进行验证;

若对所述用户账号信息和所述用户密钥均验证通过,则基于所述用户账号信息与所述用户密钥生成JWT令牌,并将所述JWT令牌发送至所述客户端。

3.根据权利要求1所述方法,其特征在于,所述JWT令牌包含加密签名和有效时长,所述对所述JWT令牌进行验证,包括:

从所述JWT令牌中获取所述加密签名和所述有效时长;

对所述加密签名进行验证,并对所述有效时长进行验证;

若对所述加密签名和所述有效时长均验证通过,则确定所述JWT令牌通过。

4.根据权利要求3所述方法,其特征在于,所述对所述有效时长进行验证,包括:

检测所述JWT令牌的生命周期,所述生命周期为所述JWT令牌的生效时间距离系统时间的时长;

若检测到所述生命周期小于所述有效时长,则确定对所述有效时长验证通过。

5.根据权利要求1-3任一项所述方法,其特征在于,所述获取预先为所述至少一个服务器中各个服务器配置的权重参数之前,所述方法还包括:

获取所述至少一个服务器中各个服务器的资源性能参数;

基于所述各个服务器的资源性能参数,分别为所述各个服务器配置权重参数。

6.根据权利要求1所述方法,其特征在于,所述基于所述散列值和所述权重参数,从所述至少一个服务器中确定出目标服务器,包括:

对所述各个服务器的权重参数进行求和运算,得到权重参数之和;

基于所述各个服务器的权重参数与所述权重参数之和,确定所述各个服务器分别对应的权重参数区间范围;

确定所述散列值与所述权重参数之和相除后的余数,并基于所述余数从所述权重参数区间范围中确定出目标权重参数区间范围;

将所述目标权重参数区间范围对应的服务器确定为所述目标服务器。

7.根据权利要求5所述方法,其特征在于,所述基于所述散列值和所述权重参数,从所述至少一个服务器中确定出目标服务器,包括:

基于所述权重参数对所述至少一个服务器中各个服务器进行排序，获得所述各个服务器的次序；

对所述各个服务器的权重参数进行求和运算，得到权重参数之和，并确定所述散列值与所述权重参数之和相除后的余数；

基于所述余数、所述各个服务器的次序以及所述各个服务器的权重参数确定出目标服务器。

8.一种访问处理装置，其特征在于，所述装置配置于网关系统对应的管理服务器，所述管理服务器用于管理至少一个服务器，所述装置包括：

获取模块，用于接收用户通过客户端发送的针对所述网关系统的访问请求，所述访问请求携带有所述用户对应的JWT令牌；

处理模块，用于对所述JWT令牌进行验证，若验证通过，则基于预设散列值规则计算所述JWT令牌对应的散列值；

所述获取模块，还用于获取预先为所述至少一个服务器中各个服务器配置的权重参数；

所述处理模块，还用于基于所述散列值和所述权重参数，从所述至少一个服务器中确定出目标服务器，并将所述访问请求发送至所述目标服务器，以使所述目标服务器对所述访问请求进行处理，并存储所述用户的操作记录。

9.一种管理服务器，其特征在于，包括处理器和存储器，所述处理器和所述存储器相互连接，其中，所述存储器用于存储计算机程序，所述计算机程序包括程序指令，所述处理器被配置用于调用所述程序指令，执行权利要求1-7任一项所述方法。

10.一种计算机可读存储介质，其特征在于，所述计算机可读存储介质存储计算机程序，所述计算机程序被处理器执行以实现权利要求1-7任意一项所述方法。

一种访问处理方法、装置及可读存储介质

技术领域

[0001] 本发明涉及计算机处理领域，尤其涉及一种访问处理方法、装置及可读存储介质。

背景技术

[0002] 在互联网业务平台对互联网业务进行处理的过程中，网关系统可以将用户通过业务平台对应的客户端提交的业务请求转发至后台服务器，使得后台服务器处理该业务请求。通常网关系统在接收到用户通过客户端发起的针对该网关系统的访问请求后，会采用随机或轮询的方式确定处理该访问请求的服务器，使得用户的操作记录分布存储于各个服务器，操作记录的连续性极低。这样的处理方式，后续若需跟踪用户操作路径，管理服务器需从各个服务器中获取并合并该用户的操作记录，操作困难，且效率低下。

[0003] 因此，如何处理用户的访问请求，以提高操作记录的连续性，成为一个亟待解决的问题。

发明内容

[0004] 本发明实施例提供了一种访问处理方法、装置及可读存储介质，采用这样的访问处理方式，可以使同一用户的访问请求被同一目标服务器处理，同一个用户的操作记录被同一个目标服务器存储，有利于提高同一用户操作记录的连续性。

[0005] 第一方面，本发明实施例提供了一种访问处理方法，所述方法应用于网关系统对应的管理服务器，所述管理服务器用于管理至少一个服务器，所述方法包括：

[0006] 接收用户通过客户端发送的针对所述网关系统的访问请求，所述访问请求携带有所述用户对应的JWT令牌；

[0007] 对所述JWT令牌进行验证，若验证通过，则基于预设散列值规则计算所述JWT令牌对应的散列值；

[0008] 获取预先为所述至少一个服务器中各个服务器配置的权重参数；

[0009] 基于所述散列值和所述权重参数，从所述至少一个服务器中确定出目标服务器，并将所述访问请求发送至所述目标服务器，以使所述目标服务器对所述访问请求进行处理，并存储所述用户的操作记录。

[0010] 第二方面，本发明实施例提供了一种访问处理装置，所述装置配置于网关系统对应的管理服务器，所述管理服务器用于管理至少一个服务器，该访问处理装置包括：

[0011] 获取模块，用于接收用户通过客户端发送的针对所述网关系统的访问请求，所述访问请求携带有所述用户对应的JWT令牌；

[0012] 处理模块，用于对所述JWT令牌进行验证，若验证通过，则基于预设散列值规则计算所述JWT令牌对应的散列值；

[0013] 所述获取模块，还用于获取预先为所述至少一个服务器中各个服务器配置的权重参数；

[0014] 所述处理模块，还用于基于所述散列值和所述权重参数，从所述至少一个服务器

中确定出目标服务器，并将所述访问请求发送至所述目标服务器，以使所述目标服务器对所述访问请求进行处理，并存储所述用户的操作记录。

[0015] 第三方面，本发明实施例提供了一种管理服务器，所述管理服务器包括输入设备和输出设备，所述管理服务器还包括处理器，适于实现一条或多条指令，所述一条或多条指令适于由所述处理器加载并执行上述第一方面所述的访问处理方法。

[0016] 第四方面，本发明实施例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中存储有指令，当其在计算机上运行时，使得计算机执行上述第一方面所述的访问处理方法。

[0017] 本申请实施例中，管理服务器可以接收用户通过客户端发送的针对该网关系统的访问请求，该访问请求中携带有用户对应的JWT令牌，管理服务器对该JWT令牌进行验证，在验证通过后，基于预设散列值规则计算该JWT令牌对应的散列值。进一步地，管理服务器可以获取预先为各个服务器配置的权重参数，并基于JWT令牌的散列值和各个服务器的权重参数从上述至少一个服务器中确定出目标服务器来处理该用户的访问请求。采用这样的访问处理方式，可以使同一用户的访问请求被同一目标服务器处理，同一个用户的操作记录被同一个目标服务器存储，有利于提高同一用户操作记录的连续性。

附图说明

[0018] 为了更清楚地说明本发明实施例或现有技术中的技术方案，下面将对实施例或现有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他的附图。

[0019] 图1是本发明实施例提供的一种访问处理系统的架构示意图；

[0020] 图2是本发明实施例提供的一种访问处理方法的流程示意图；

[0021] 图3是本发明实施例提供的另一种访问处理方法的流程示意图；

[0022] 图4是本发明实施例提供的一种访问处理装置的结构示意图；

[0023] 图5是本发明实施例提供的一种管理服务器的结构示意图。

具体实施方式

[0024] 下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

[0025] 请参见图1，是本发明实施例提供的一种访问处理系统的架构示意图，该访问处理系统包括用户操作的客户端10，管理服务器11，服务器集群12。其中：

[0026] 用户操作的客户端10和管理服务器11具体可以为智能手机、平板电脑、笔记本电脑、台式电脑、车载智能终端等，本发明实施例不做限定。服务器集群12中可以包括多台服务器121，每台服务器121在进行正常工作时可以接收管理服务器11发送的访问请求，并处理该访问请求。需要说明的是，服务器集群12中的所示的服务器数目仅仅示意性的，根据实际需要，可以部署任意数目的服务器。

[0027] 在一些可行的实施方式中，管理服务器11接收用户通过客户端10发送的携带有(JSON Web Token，JWT)令牌的访问请求，并对该访问请求中的JWT令牌进行验证，验证通过后计算该JWT令牌的散列值，进一步地，管理服务器11可以基于该散列值与预先为各台服务器121配置的权重参数从至少一个服务器中确定出目标服务器，并将该访问请求转发至目标服务器，以使该目标服务器处理上述访问请求。由于同一用户的访问请求对应的JWT令牌的散列值相同，则通过JWT令牌的散列值选定的目标服务器相同，采用这样的访问处理方式，可以使同一用户的访问请求被同一目标服务器处理，同一个用户的操作记录被同一个目标服务器存储，有利于提高同一用户操作记录的连续性。

[0028] 其中，JWT令牌一个开放式表针，它定义了一种紧凑且字包含的方式，并使得通信各方之间以JSON对象安全传输信息。JWT令牌由三个部分组成，分别是头部(Header)、负载部分(Payload)和加密签名(Signature)。其中，Header通常由令牌类型和加密的哈希算法两部分组成，Payload中存放着JWT令牌的有效信息，Signature是JWT令牌的加密签名，主要用于防止JWT内容被篡改。

[0029] 以下对本发明实施例的技术方案的实现细节进行详细阐述:

[0030] 请参见图2，是本发明实施例提供的一种访问处理方法的流程示意图，该方法应用于网关系统对应的管理服务器，该管理服务器用于管理至少一个服务器，该访问处理方法包括如下步骤：

[0031] S201:接收用户通过客户端发送的针对该网关系统的访问请求，该访问请求中携带有用户对应的JWT令牌。

[0032] 其中，上述客户端可以是上述管理服务器上的客户端，也可以是除管理服务器以外的其他手机、平板电脑、笔记本电脑、台式电脑等前端设备上的客户端。

[0033] 具体地，用户从客户端发起针对该网关系统的访问请求，客户端针对该访问请求从本地存储、Cookie或后端服务器中调用JWT令牌，并将该JWT令牌添加至访问请求中，进而将添加了JWT令牌的访问请求发送至网关系统对应的管理服务器。

[0034] 在一个实施例中，管理服务器在接收用户通过客户端发送的针对该网关系统的访问请求之前，还可以接收用户通过客户端提交的用户账号信息和用户密钥，并对该用户账号信息和用户密钥进行验证，若对该用户账号信息和用户密钥均验证通过，则基于该用户账号信息与用户密钥生成JWT令牌，并将该JWT令牌发送至上述客户端。

[0035] 具体地，用户通过客户端向管理服务器提交该用户账号信息和用户密钥，其中，该用户账号信息可以为用户名、用户手机号码和用户邮箱中的一种或多种。管理服务器接收该用户账号信息和用户密钥，并获取用户注册表，该用户注册表中存储有用户注册时上传的用户账号信息和用户密钥，进一步地，管理服务器可以将用户提交的用户账号信息和用户注册表中预先存储的用户账号信息进行比对，若两者比对结果相同，则确定该用户提交的用户账号信息验证通过。并且，管理服务器还可以将用户提交的用户密钥与用户注册表中预先存储的用户账号信息对应的用户密钥进行对比，若两者对比结果相同，则确定对该用户提交的用户密钥验证通过。

[0036] 若对该用户账号信息和用户密钥均验证通过，则基于该用户账号信息与用户密钥生成JWT令牌，即该JWT令牌的负载中包含有用户账号信息和用户密钥中的一种或两种。

[0037] 若管理服务器将用户提交的用户账号信息和用户注册表中预先存储的用户账号

信息进行比对，两者对比结果不相同，则确定对用户账号信息验证不通过，管理服务器向客户端发出用户账号信息不正确的提示，以提示用户更正提交的用户账号信息。若管理服务器将用户提交的用户密钥与用户注册表中预先存储的用户账号信息对应的用户密钥进行对比，两者对比结果不相同，则确定对用户密钥验证不通过，管理服务器向客户端发出用户密钥错误的提示，以提示用户更正提交的用户密钥或用户账号信息。

[0038] S202：对上述JWT令牌进行验证，若验证通过，则基于预设散列值规则计算该JWT令牌对应的散列值。

[0039] 其中，预设散列值规则可以是散列算法，由开发人员设定，后期可根据实际情况进行调整。通过散列算法计算出来的散列值为一个短的字符串，该字符串由随机字母和数字组成，并且，该散列算法对相同的数据进行运算得到的散列值结果相同。该预设散列值规则可如下所示：

[0040] $hash=s[0]\times31^{n-1}+s[1]\times31^{n-2}+...+s[n-1]$

[0041] 其中，s为JWT令牌中用户唯一标识的ascii编码数组，n为ascii编码数组中字符长度，s[0]为acsii数组中第一个数字，s[1]为acsii数组中第二个数字，s[n-1]为acsii数组中第n个数字。

[0042] 具体地，管理服务器从访问请求中获取JWT令牌，对JWT令牌进行验证，该验证内容包括验证JWT令牌的有效性和验证JWT令牌的真实性，验证JWT令牌的真实性即验证JWT令牌是否是由网关系统认证颁发，验证JWT令牌的有效性既是验证该JWT令牌是否处于有效期内。管理服务器对JWT令牌验证通过后，利用预设散列值规则对JWT令牌的负载中用户标识信息(如用户账号信息)进行计算，得到该JWT令牌对应的散列值，采用这种方式，以保证同一用户的JWT令牌的散列值一致。

[0043] 在一个实施例中，该JWT令牌包含有加密签名和有效时长，管理服务器从该JWT令牌中获取该加密签名和有效时长，进一步地，管理服务器可以对该加密签名和该有效时长进行验证。若对该加密签名和有效时长均验证通过，则确定该JWT令牌通过。

[0044] 其中，该加密签名是由管理服务器在生成JWT令牌时，为了防止该JWT令牌被篡改而生成的数字签名。有效时长的设置可以防止JWT令牌中信息泄露，该有效时长的具体数值由开发人员根据实验数据测算得到的，后续可以根据实际情况进行调整。

[0045] 在一个实施例中，管理服务器可以检测该JWT令牌的生命周期，其中，生命周期为JWT令牌的生效时间距离系统时间的时长。若管理服务器检测到上述生命周期小于该有效时长，则确定对有效时长验证通过。

[0046] 若管理服务器检测到上述生命周期大于或等于该有效时长，则判定对有效时长的验证不通过。管理服务器向用户对应的客户端发出提示信息，以提示用户提交用户账号信息和用户密钥生成新的JWT令牌，并对该新的JWT令牌进行验证。

[0047] 在一个实施例中，管理服务器获取JWT令牌的加密签名，并采用管理服务器中预先存储的密钥对该加密签名进行解密，若解密成功，则确定该加密签名验证通过。若解密失败，则确定该加密签名验证失败，并判定该JWT令牌已被非法篡改。管理服务器向用户对应的客户端发出提示信息，以提示用户提交用户账号信息和用户密钥生成新的JWT令牌，并对该新的JWT令牌进行验证。

[0048] 其中，预先存储的密钥是管理服务器在生成该JWT令牌的加密签名时生成的密钥，

该密钥可以是采用对称加密时的公钥,也可以是非对称加密时的私钥。

[0049] S203:获取预先为至少一个服务器中各个服务器配置的权重参数。

[0050] 其中,该权重参数可以是开发人员根据实验数据测算后进行配置,也可以是管理服务器根据预设权重参数的规则进行设置,预设权重参数规则可以是根据各台服务器的资源性能参数设定权重参数的规则,也可以是根据各台服务器业务功能设置权重参数的规则,在此不做具体限定。

[0051] S204:基于该散列值和权重参数,从上述至少一个服务器中确定出目标服务器,并将该访问请求发送至目标服务器,以使目标服务器对该访问请求进行处理,并存储该用户的操作记录。

[0052] 管理服务器基于预设计算规则对上述散列值和权重参数进行计算,并根据计算结果确定该散列值对应的服务器,将该服务器确定为目标服务器,并将该访问请求发送至目标服务器,以使目标服务器对该访问请求进行处理,存储该用户的操作记录。其中,预设计算规则可以是数值运算规则。由于散列值是根据JWT令牌中用户标识(如用户账号信息)计算得到,故同一用户对应同一散列值,而同一散列值和各个服务器的权重参数进行计算将会得到同样的计算结果,即选择同一目标服务器,采用这样的访问处理方式,可以使同一用户的访问请求被同一目标服务器处理,同一个用户的操作记录被同一个目标服务器存储,进而保证操作记录的连续性。

[0053] 本申请实施例中,管理服务器可以接收用户通过客户端发送的针对该网关系统的访问请求,该访问请求中携带有用户对应的JWT令牌,进而,管理服务器可以对该JWT令牌进行验证,若验证通过,则基于预设散列值规则计算该JWT令牌对应的散列值,并获取预先为至少一个服务器中各个服务器配置的权重参数,进一步地,管理服务器可以基于该散列值和权重参数从至少一个服务器中确定出目标服务器,并将该访问请求发送至目标服务器,以使目标服务器对该访问请求进行处理,并存储该用户的操作记录。采用这样的访问处理方法,可以使同一用户的访问请求被同一目标服务器处理,同一个用户的操作记录被同一个目标服务器存储,有利于提高同一用户操作记录的连续性。

[0054] 请参见图3,是本发明实施例提供的另一种访问处理方法的流程示意图,该访问处理方法包括如下步骤:

[0055] S301:接收用户通过客户端发送的针对该网关系统的访问请求,该访问请求中携带有用户对应的JWT令牌。

[0056] S302:对上述JWT令牌进行验证,若验证通过,则基于预设散列值规则计算该JWT令牌对应的散列值。

[0057] 其中,步骤S301-S302的具体实现过程可参见前述实施例步骤S201-S202中的具体描述,此处不再对其进行赘述。

[0058] S303:获取至少一个服务器中各个服务器的资源性能参数。

[0059] 其中,资源性能参数包括服务器CPU运行速率、内存容量和吞吐量大小等等。在各个服务器在处于初始运行状态时,管理服务器分别获取各个服务器的资源性能参数。

[0060] S304:基于各个服务器的资源性能参数,分别为各个服务器配置权重参数。

[0061] 管理服务器根据基于各个服务器的资源性能参数和权重参数的配置规则,分别为各个服务器配置权重参数。其中,该权重参数的配置规则由开发人员设定,可以根据实际情

况进行调整。

[0062] 示例性地，网关系统对应的管理服务器管理的服务器有A服务器和B服务器，在A服务器和B服务器均处于初始运行状态时，管理服务器获取A服务器的资源性能参数为：内存容量为8G，吞吐量的大小为3000kps；管理服务器获取B服务器的资源性能参数为：内存容量为4G，吞吐量的大小为2000kps。则根据表1所示的基于内存容量的评分准则对各个服务器进行评分，该评分结果为：A服务器得3分，B服务器得2分；根据表2所示的基于吞吐量性能的评分准则对各个服务器进行评分，该评分结果为：A服务器得3分，B服务器的2分。故管理服务器为A服务器配置权重参数为3+3＝6，为B服务器配置权重参数为2+2＝4。

[0063] 表1

[0064]

内存容量性能评分准则	
内存容量（x）	评分
x>16G	4 分
4G<x=<16G	3 分
2G<x=<4G	2 分
x=<2G	1 分

[0065] 表2

[0066]

吞吐量性能评分准则	
吞吐量大小(y)	评分
y >3000kps	4 分
2001kps< y =<3000kps	3 分
1001kps< y =<2000kps	2 分
0kps< y =<1000kps	1 分

[0067] S305：获取预先为至少一个服务器中各服务器配置的权重参数。

[0068] 其中，步骤S305的具体实现过程可参见前述实施例步骤S203的具体描述，此处不再对其进行赘述。

[0069] S306：基于该散列值和权重参数，从上述至少一个服务器中确定出目标服务器，并将该访问请求发送至目标服务器，以使目标服务器对该访问请求进行处理，并存储该用户的操作记录。

[0070] 在一个实施例中，管理服务器可以对各个服务器的权重参数进行求和运算，得到权重之后，进而可以基于各个服务器的权重参数与权重参数之和，确定各个服务器分别对应的权重参数区间范围。进一步地，管理服务器确定上述散列值与权重参数之和相除后的余数，进而基于该余数从该权重参数区间范围中确定出目标权重参数区间范围，将该目标权重参数区间范围对应的服务器确定为目标服务器，并将该访问请求发送至目标服务器，

以使目标服务器对该访问请求进行处理，并存储该用户的操作记录。

[0071] 示例性地，用户的JWT令牌的散列值为1000，网关系统对应的管理服务器管理有a、b、c三台服务器，a服务器的权重参数为100，b服务器的权重参数为20，c服务器的权重参数为10，权重参数之和为130，则确定总权重参数区间范围为0-130，a服务器对应的权重参数区间范围为0-100，b服务器对应的权重参数区间范围为100-120，c服务器对应的权重参数区间范围为120-130。管理服务器确定散列值与权重参数之和相除后的余数为90，进一步地，管理服务器确定余数90落到a服务器对应的权重参数区间范围为0-100中，故管理服务器将a服务器确定为目标服务器，并向a服务器转发上述访问请求，以使a服务器对该访问请求进行处理，并存储该用户的操作记录。

[0072] 在另一个实施例中，管理服务器基于权重参数对至少一个服务器中各个服务器进行排序，获得各个服务器的次序，并对各个服务器的权重参数进行求和运算，得到权重参数之和，进而确定该散列值与权重参数之和相除后的余数。进一步地，管理服务器基于该余数、各个服务器的次序以及各个服务器的权重参数确定出目标服务器，并将该访问请求发送至目标服务器，以使目标服务器对该访问请求进行处理，并存储该用户的操作记录。

[0073] 示例性地，用户的JWT令牌的散列值为1000，网关系统对应的管理服务器管理有a、b、c三台服务器，a服务器的权重参数为100，b服务器的权重参数为20，c服务器的权重参数为10，权重参数之和为130。进一步地，管理服务器基于权重参数对各个服务器进行从大到小的排序，得到各个服务器的次序，并确定散列值与权重参数之和相除后的余数为90。管理服务器将该余数基于各个服务器的次序，与各个服务器的权重参数依次相减，直到该差值小于或等于0，则管理服务器将最后一次相减权重参数对应的服务器确定为目标服务器，在本示例中，余数90与排序第一的a服务器的权重参数100相减的差值为-10，该差值小于0，则管理服务器将a服务器确定为目标服务器，并向a服务器转发上述访问请求，以使a服务器对该访问请求进行处理，并存储该用户的操作记录。

[0074] 在一个实施例中，管理服务器将上述访问请求发送至目标服务器后，目标服务器从该访问请求中获取用户的用户信息，并记录该用户的操作记录，将该操作记录与该用户的用户信息关联存储至数据库中。

[0075] 示例性的，管理服务器将用户A的访问请求发送至服务器a，服务器a记录用户A的操作记录，并将该操作记录与用户A信息关联存储至数据库中，如表3所示：

[0076] 表3

[0077]

用户A
操作记录1
操作记录2
操作记录3
操作记录4

[0078] 在一个实施例中，管理服务器将上述访问请求发送至目标服务器后，将该用户信息与处理上述访问请求的目标服务器信息进行关联存储至数据库中。管理服务器接收针对用户的路径跟踪请求，该路径跟踪请求中携带有用户信息，进一步地，管理服务器可以基于该用户信息从数据库中查询获得该用户信息对应的目标服务器信息，并从该目标服务器中获取该用户的操作记录。由于本申请实施例提出的访问处理方法，可以保证同一用户的访

问请求被同一个目标服务器处理，也即，同一用户的操作记录被存储于同一个目标服务器。这种情况下，当需要对任一用户进行路径跟踪时，可以直接从该用户对应的目标服务器中获取该用户的操作记录，而无需去其它服务器获取，可以提高该用户的操作记录的获取效率，进而有利于提高该用户的路径跟踪效率。

[0079] 示例性地，管理服务器将用户A的访问请求发送至服务器a，将用户B的访问请求发送至服务器a，将用户C的访问请求发送至服务器b，并将上述用户信息与处理该访问请求的目标服务器信息进行关联存储至数据库中，如表4所示：

[0080] 表4

[0081]

用户信息	目标服务器信息
用户A	服务器a
用户B	服务器a
用户C	服务器b

[0082] 当管理服务器接收到针对用户A的路径跟踪请求，管理服务器可以根据用户A信息从数据库中查询获得处理用户A访问请求的服务器a，并从服务器a的数据库中获得如表3所示的用户A的操作记录。由于采用本申请实施例提出的访问处理方法，同一用户的访问请求被同一个目标服务器处理，也即，同一用户的操作记录被存储于同一个目标服务器。这种情况下，当需要对用户A进行路径跟踪时，可以直接从该用户A对应的目标服务器中获取该用户A的操作记录，而无需去其它服务器获取，可以提高用户A的操作记录的获取效率，进而有利于提高针对用户A的路径跟踪的效率。

[0083] 本申请实施例中，管理服务器可以接收用户通过客户端发送的针对该网关系统且携带有用户对应的JWT令牌的访问请求，并对该JWT令牌进行验证，若验证通过，则基于预设散列值规则计算该JWT令牌对应的散列值。管理服务器还可以获取至少一个服务器中各个服务器的资源性能参数，并基于各个服务器的资源性能参数，分别为各个服务器配置权重参数，进一步地，管理服务器可以获取预先为至少一个服务器中各服务器配置的权重参数，并基于该散列值和权重参数从上述至少一个服务器中确定出目标服务器，并将该访问请求发送至目标服务器，以使目标服务器对该访问请求进行处理，并存储该用户的操作记录。采用这样的访问处理方式，可以使同一用户的访问请求被同一目标服务器处理，同一个用户的操作记录被同一个目标服务器存储，有利于提高同一用户操作记录的连续性。

[0084] 基于上述方法实施例的描述，本发明实施例还提出了一种访问处理装置，该装置应用于网关系统对应的管理服务器，该管理服务器用于管理至少一个服务器。请参见图4所示，该访问处理装置包括如下模块：

[0085] 获取模块40，用于接收用户通过客户端发送的针对所述网关系统的访问请求，所述访问请求携带有所述用户对应的JWT令牌；

[0086] 处理模块41，用于对所述JWT令牌进行验证，若验证通过，则基于预设散列值规则计算所述JWT令牌对应的散列值；

[0087] 所述获取模块40，还用于获取预先为所述至少一个服务器中各个服务器配置的权重参数；

[0088] 所述处理模块41，还用于基于所述散列值和所述权重参数，从所述至少一个服务器中确定出目标服务器，并将所述访问请求发送至所述目标服务器，以使所述目标服务器

对所述访问请求进行处理，并存储所述用户的操作记录。

[0089] 在一个实施例中，所述处理模块41在接收用户通过客户端发送的针对所述网关系统的访问请求之前，具体还用于：

[0090] 接收用户通过客户端提交的用户账号信息和用户密钥，并对所述用户账号信息和所述用户密钥进行验证；

[0091] 若对所述用户账号信息和所述用户密钥均验证通过，则基于所述用户账号信息与所述用户密钥生成JWT令牌，并将所述JWT令牌发送至所述客户端。

[0092] 在一个实施例中，所述处理模块41在JWT令牌包含加密签名和有效时长，在对所述JWT令牌进行验证时，具体可以用于：

[0093] 从所述JWT令牌中获取所述加密签名和所述有效时长；

[0094] 对所述加密签名进行验证，并对所述有效时长进行验证；

[0095] 若对所述加密签名和所述有效时长均验证通过，则确定所述JWT令牌通过。

[0096] 在一个实施例中，所述处理模块41在对所述有效时长进行验证时，具体可以用于：

[0097] 检测所述JWT令牌的生命周期，所述生命周期为所述JWT令牌的生效时间距离系统时间的时长；

[0098] 若检测到所述生命周期小于所述有效时长，则确定对所述有效时长验证通过。

[0099] 在一个实施例中，所述处理模块41在获取预先为所述至少一个服务器中各个服务器配置的权重参数之前，具体还可以用于：

[0100] 获取所述至少一个服务器中各个服务器的资源性能参数；

[0101] 基于所述各个服务器的资源性能参数，分别为所述各个服务器配置权重参数。

[0102] 在一个实施例中，所述处理模块41在基于所述散列值和所述权重参数，从所述至少一个服务器中确定出目标服务器时，具体可以用于：

[0103] 对所述各个服务器的权重参数进行求和运算，得到权重参数之和；

[0104] 基于所述各个服务器的权重参数与所述权重参数之和，确定所述各个服务器分别对应的权重参数区间范围；

[0105] 确定所述散列值与所述权重参数之和相除后的余数，并基于所述余数从所述权重参数区间范围中确定出目标权重参数区间范围；

[0106] 将所述目标权重参数区间范围对应的服务器确定为所述目标服务器。

[0107] 在一个实施例中，所述处理模块41在基于所述散列值和所述权重参数，从所述至少一个服务器中确定出目标服务器时，具体可以用于：

[0108] 基于所述权重参数对所述至少一个服务器中各个服务器进行排序，获得所述各个服务器的次序；

[0109] 对所述各个服务器的权重参数进行求和运算，得到权重参数之和，并确定所述散列值与所述权重参数之和相除后的余数；

[0110] 基于所述余数、所述各个服务器的次序以及所述各个服务器的权重参数确定出目标服务器。

[0111] 需要说明的是，本发明实施例所描述的访问处理装置的各模块的功能可根据图2或图3所述的方法实施例中的方法具体实现，其具体实现过程可以参照图2或图3方法实施例的相关描述，此处不再赘述。

[0112] 基于上述方法实施例以及装置项实施例的描述，本发明实施例还提供一种管理服务器。请参见图5，该管理服务器可至少包括处理器501、输入设备502、输出设备503以及存储器504；其中，处理器501、输入设备502、输出设备503以及存储器504可通过总线或者其它连接方式进行连接。所述存储器504用于存储计算机程序，所述计算机程序包括程序指令，所述处理器501用于执行所述存储器504存储的程序指令。处理器501(或称CPU(Central Processing Unit，中央处理器))是管理服务器的计算核心以及控制核心，其适于实现一条或多条指令，具体适于加载并执行一条或多条指令从而实现上述访问处理方法实施例中的相应方法流程或相应功能。其中，处理器501被配置调用所述程序指令执行：接收用户通过客户端发送的针对所述网关系统的访问请求，所述访问请求携带有所述用户对应的JWT令牌；对所述JWT令牌进行验证，若验证通过，则基于预设散列值规则计算所述JWT令牌对应的散列值；获取预先为所述至少一个服务器中各个服务器配置的权重参数；基于所述散列值和所述权重参数，从所述至少一个服务器中确定出目标服务器，并将所述访问请求发送至所述目标服务器，以使所述目标服务器对所述访问请求进行处理，并存储所述用户的操作记录。

[0113] 在一个实施例中，所述处理器501在接收用户通过客户端发送的针对所述网关系统的访问请求之前，具体还用于：

[0114] 接收用户通过客户端提交的用户账号信息和用户密钥，并对所述用户账号信息和所述用户密钥进行验证；

[0115] 若对所述用户账号信息和所述用户密钥均验证通过，则基于所述用户账号信息与所述用户密钥生成JWT令牌，并将所述JWT令牌发送至所述客户端。

[0116] 在一个实施例中，所述处理器501在JWT令牌包含加密签名和有效时长，在对所述JWT令牌进行验证时，具体可以用于：

[0117] 从所述JWT令牌中获取所述加密签名和所述有效时长；

[0118] 对所述加密签名进行验证，并对所述有效时长进行验证；

[0119] 若对所述加密签名和所述有效时长均验证通过，则确定所述JWT令牌通过。

[0120] 在一个实施例中，所述处理器501在对所述有效时长进行验证时，具体可以用于：

[0121] 检测所述JWT令牌的生命周期，所述生命周期为所述JWT令牌的生效时间距离系统时间的时长；

[0122] 若检测到所述生命周期小于所述有效时长，则确定对所述有效时长验证通过。

[0123] 在一个实施例中，所述处理器501在获取预先为所述至少一个服务器中各个服务器配置的权重参数之前，具体还可以用于：

[0124] 获取所述至少一个服务器中各个服务器的资源性能参数；

[0125] 基于所述各个服务器的资源性能参数，分别为所述各个服务器配置权重参数。

[0126] 在一个实施例中，所述处理器501在基于所述散列值和所述权重参数，从所述至少一个服务器中确定出目标服务器时，具体可以用于：

[0127] 对所述各个服务器的权重参数进行求和运算，得到权重参数之和；

[0128] 基于所述各个服务器的权重参数与所述权重参数之和，确定所述各个服务器分别对应的权重参数区间范围；

[0129] 确定所述散列值与所述权重参数之和相除后的余数，并基于所述余数从所述权重

参数区间范围中确定出目标权重参数区间范围；

[0130] 将所述目标权重参数区间范围对应的服务器确定为所述目标服务器。

[0131] 在一个实施例中，所述处理器501在基于所述散列值和所述权重参数，从所述至少一个服务器中确定出目标服务器时，具体可以用于：

[0132] 基于所述权重参数对所述至少一个服务器中各个服务器进行排序，获得所述各个服务器的次序；

[0133] 对所述各个服务器的权重参数进行求和运算，得到权重参数之和，并确定所述散列值与所述权重参数之和相除后的余数；

[0134] 基于所述余数、所述各个服务器的次序以及所述各个服务器的权重参数确定出目标服务器。

[0135] 应当理解，在本发明实施例中，所称处理器501可以是中央处理单元(Central Processing Unit,CPU)，该处理器501还可以是其他通用处理器、数字信号处理器(Digital Signal Processor,DSP)、专用集成电路(Application Specific Integrated Circuit,ASIC)、现成可编程门阵列(Field-Programmable Gate Array,FPGA)或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立a硬件组件等。通用处理器可以是微处理器或者该处理器也可以是任何常规的处理器等。

[0136] 该存储器504可以包括只读存储器和随机存取存储器，并向处理器501提供指令和数据。存储器504的一部分还可以包括非易失性随机存取存储器。例如，存储器504还可以存储设备类型的信息。该输入设备502可以包括触控板、指纹采传感器(用于采集用户的指纹信息)、麦克风、实体键盘等，输出设备503可以包括显示器(LCD等)、扬声器等。

[0137] 具体实现中，本发明实施例中所描述的处理器501、存储器504、输入设备502和输出设备503可执行本发明实施例提供的图2或者图3所述的方法实施例所描述的实现方式，也可执行本发明实施例图4所描述的访问处理装置的实现方法，在此不再赘述。

[0138] 在本发明的另一实施例中提供一种计算机可读存储介质，所述计算机可读存储介质存储有计算机程序，所述计算机程序包括程序指令，所述程序指令被处理器执行时实现本发明实施例提供的图2或者图3所述的方法实施所描述的实现方式，所述计算机可读存储介质可以是前述任一实施例所述的管理服务器的内部存储单元，例如管理服务器的硬盘或内存。所述计算机可读存储介质也可以是所述管理服务器的外部存储设备，例如所述管理服务器上配备的插接式硬盘，智能存储卡(Smart Media Card,SMC)，安全数字(Secure Digital,SD)卡，闪存卡(Flash Card)等。进一步地，所述计算机可读存储介质还可以既包括所述管理服务器的内部存储单元也包括外部存储设备。所述计算机可读存储介质用于存储所述计算机程序以及所述管理服务器所需的其他程序和数据。所述计算机可读存储介质还可以用于暂时地存储已经输出或者将要输出的数据。

[0139] 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，所述的程序可存储于一计算机可读取可读存储介质中，该程序在执行时，可包括如上述各方法的实施例的流程。

[0140] 其中，所述的可读存储介质可为磁碟、光盘、只读存储记忆体(Read-Only Memory,ROM)或随机存储记忆体(Random Access Memory,RAM)等。

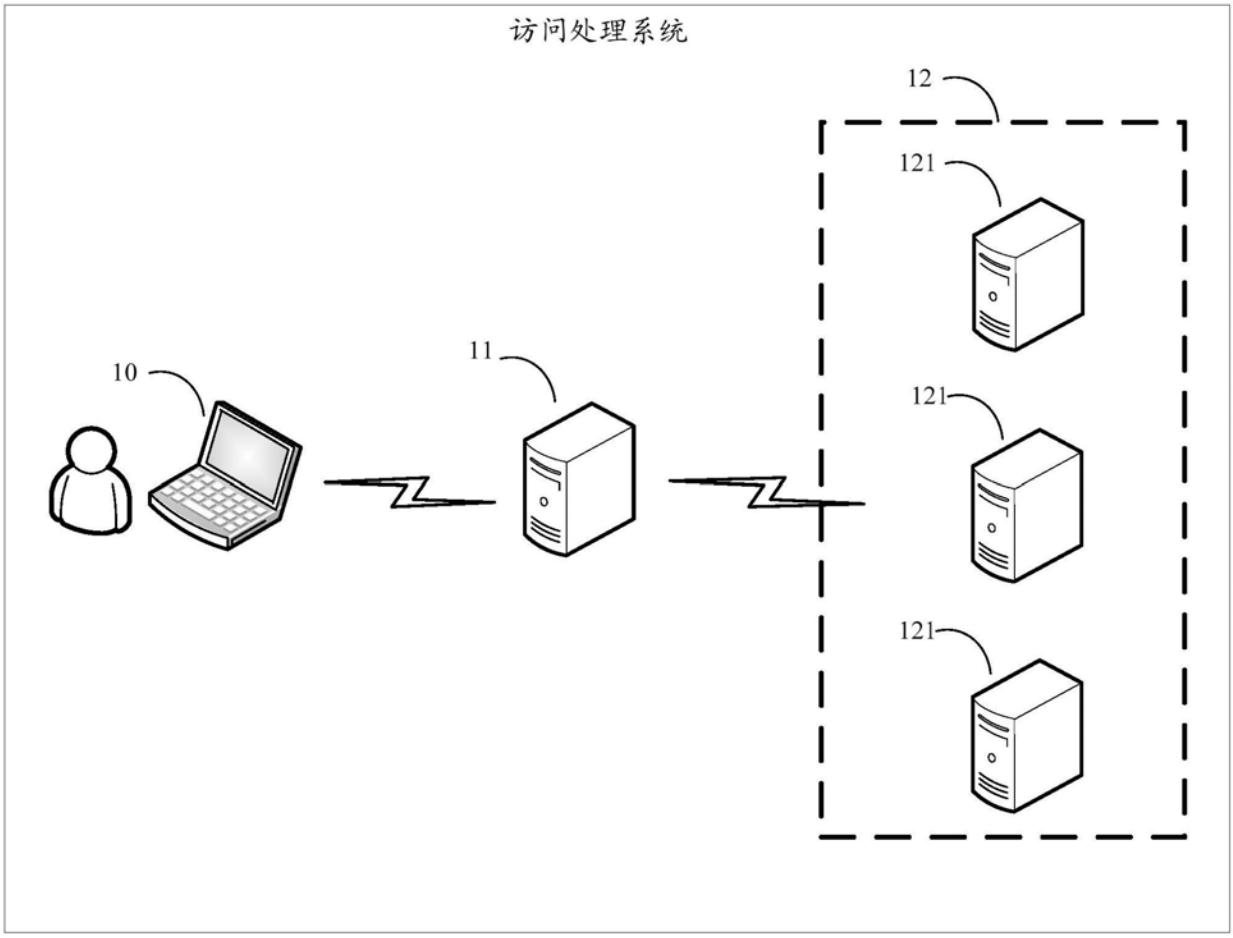


图1

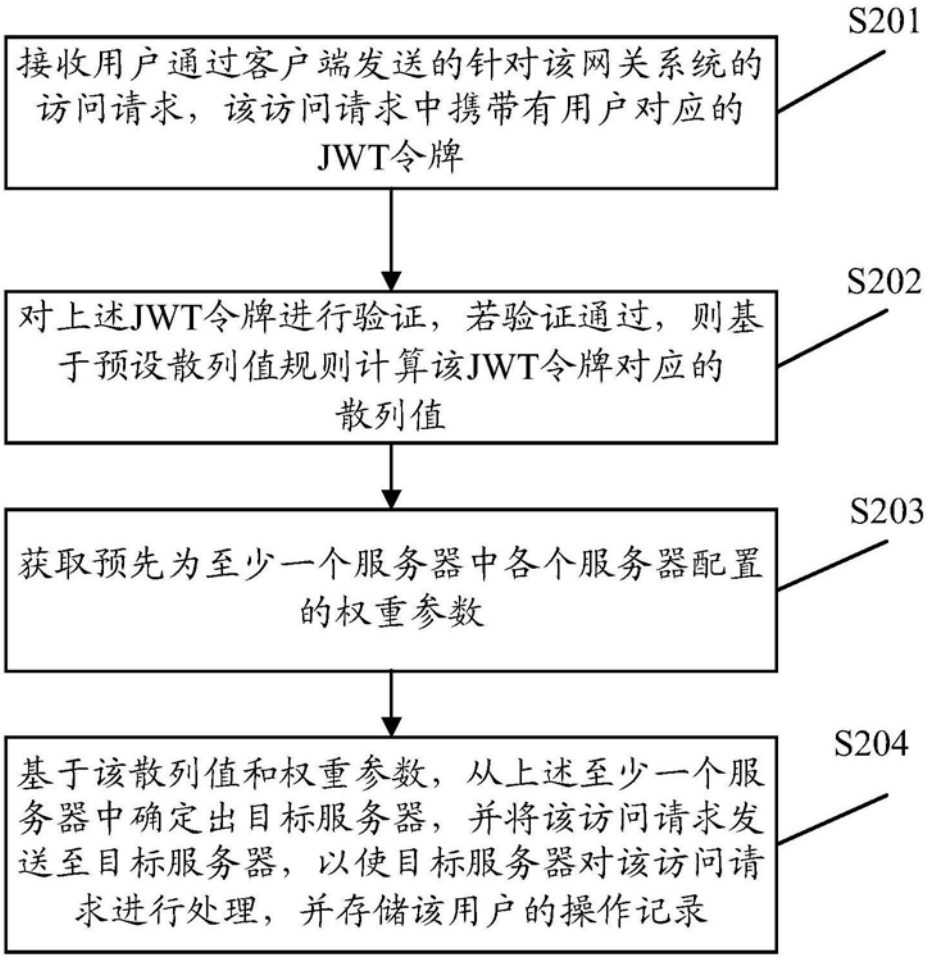

S201
接收用户通过客户端发送的针对该网关系统的访问请求，该访问请求中携带有用户对应的JWT令牌
S202
对上述JWT令牌进行验证，若验证通过，则基于预设散列值规则计算该JWT令牌对应的散列值
S203
获取预先为至少一个服务器中各个服务器配置的权重参数
S204
基于该散列值和权重参数，从上述至少一个服务器中确定出目标服务器，并将该访问请求发送至目标服务器，以使目标服务器对该访问请求进行处理，并存储该用户的操作记录

图2

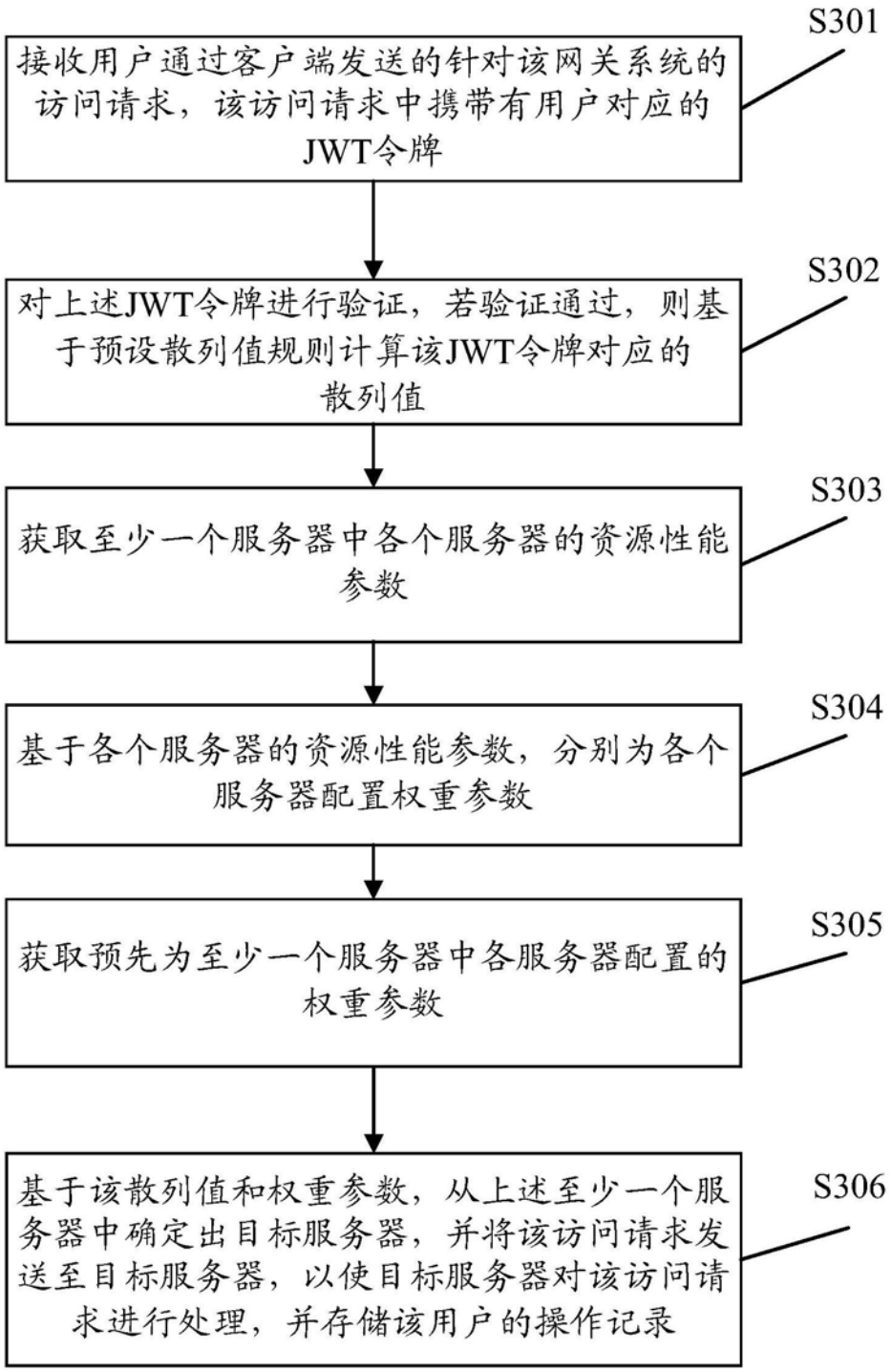

S301
接收用户通过客户端发送的针对该网关系统的访问请求，该访问请求中携带有用户对应的JWT令牌
S302
对上述JWT令牌进行验证，若验证通过，则基于预设散列值规则计算该JWT令牌对应的散列值
S303
获取至少一个服务器中各个服务器的资源性能参数
S304
基于各个服务器的资源性能参数，分别为各个服务器配置权重参数
S305
获取预先为至少一个服务器中各服务器配置的权重参数
S306
基于该散列值和权重参数，从上述至少一个服务器中确定出目标服务器，并将该访问请求发送至目标服务器，以使目标服务器对该访问请求进行处理，并存储该用户的操作记录

图3

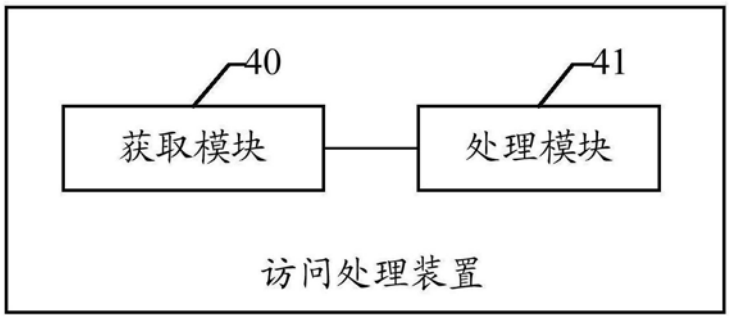

40
41
获取模块
处理模块
访问处理装置

图4

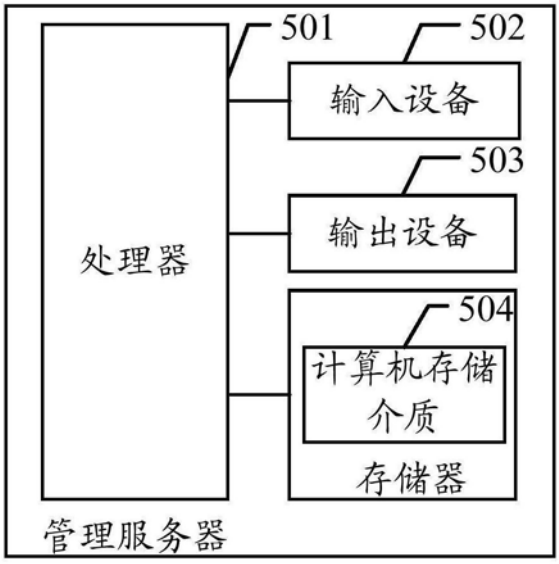

501
502
输入设备
503
输出设备
处理器
504
计算机存储介质
存储器
管理服务器

图5