(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 111800390 A
(43)申请公布日 2020.10.20

(21)申请号 202010538249.3

(22)申请日 2020.06.12

(71)申请人 深信服科技股份有限公司
地址 518055 广东省深圳市南山区学苑大道1001号南山智园A1栋

(72)发明人 夏威夷 卢艺

(74)专利代理机构 北京派特恩知识产权代理有限公司 11270
代理人 贾伟 张颖玲

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 9/32(2006.01)
H04L 29/08(2006.01)

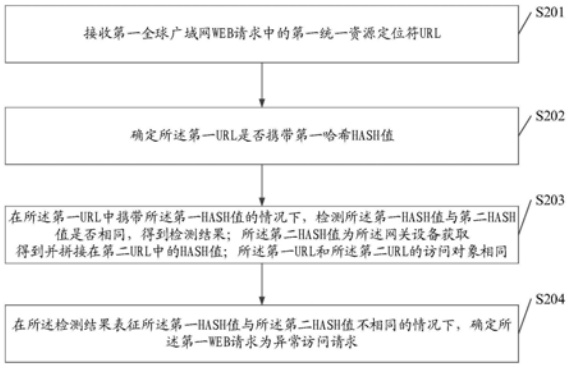
权利要求书2页 说明书11页 附图5页

(54)发明名称

异常访问检测方法、装置、网关设备及存储介质

(57)摘要

本发明实施例适用于通信技术领域，提供了一种异常访问检测方法、装置、网关设备及存储介质，其中，异常访问检测包括：接收第一全球广域网WEB请求中的第一统一资源定位符URL；确定所述第一URL是否携带第一哈希HASH值；在所述第一URL中携带所述第一HASH值的情况下，检测所述第一HASH值与第二HASH值是否相同，得到检测结果；所述第二HASH值为所述网关设备获取得到并拼接在第二URL中的HASH值；所述第一URL和所述第二URL的访问对象相同；在所述检测结果表征所述第一HASH值与所述第二HASH值不相同的情况下，确定所述第一WEB请求为异常访问请求。



CN 111800390 A

1.一种异常访问检测方法,应用于网关设备,其特征在于,所述方法包括:

接收第一全球广域网WEB请求中的第一统一资源定位符URL;

确定所述第一URL是否携带第一哈希HASH值;

在所述第一URL携带所述第一HASH值的情况下,检测所述第一HASH值与第二HASH值是否相同,得到检测结果;所述第二HASH值为所述网关设备获取得到并拼接在第二URL中的HASH值;所述第一URL和所述第二URL的访问对象相同;

在所述检测结果表征所述第一HASH值与所述第二HASH值不相同的情况下,确定所述第一WEB请求为异常访问请求。

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:

在所述第一URL未携带所述第一HASH值的情况下,确定所述第一URL是否在设定的第一数据表中;当所述第一URL存储于所述第一数据表时,对应的所述第一WEB请求为正常访问请求;

在所述第一URL不在所述设定的第一数据表中的情况下,确定所述第一WEB请求为异常访问请求。

3.根据权利要求2所述的方法,其特征在于,在接收第一WEB请求之前,所述方法还包括:

确定所述第一数据表;

所述确定所述第一数据表,包括:

接收关于所述访问对象的第二WEB请求;所述第二WEB请求中的第三URL未携带HASH值;

根据接收到的所述第二WEB请求,确定发起所述第二WEB请求的用户数量;

在所述用户数量大于设定值的情况下,将所述第三URL写入所述第一数据表。

4.根据权利要求3所述的方法,其特征在于,所述根据接收到的所述第二WEB请求,确定发起所述第二WEB请求的用户数量时,所述方法包括:

在第一次接收到所述第二WEB请求时,将所述第三URL写入第二数据表中,并根据接收到的所述第二WEB请求实时更新所述第二数据表中所述第三URL对应的用户数量。

5.根据权利要求1所述的方法,其特征在于,所述方法还包括:

基于第四URL获取所述第二HASH值;

将所述第二HASH值拼接在所述第四URL中,得到所述第二URL,以使终端设备根据所述第二URL访问所述访问对象;其中,

所述第四URL为所述访问对象对应的资源地址。

6.根据权利要求5所述的方法,其特征在于,所述基于第四URL获取所述第二HASH值,包括:

基于所述第四URL和设定信息获取所述第二HASH值;所述设定信息至少包括所述终端设备登录所述网关设备时对应的随机码。

7.根据权利要求6所述的方法,其特征在于,所述设定信息还包括以下任意一项或多项:

所述终端设备登录所述网关设备时使用的用户信息;

所述终端设备访问所述访问对象的WEB请求中携带的密钥。

8.一种异常访问检测装置,其特征在于,包括:

接收模块，用于接收第一WEB请求中的第一URL；

第一确定模块，用于确定所述第一URL是否携带第一HASH值；

检测模块，用于在所述第一URL中携带所述第一HASH值的情况下，检测所述第一HASH值与第二HASH值是否相同，得到检测结果；所述第二HASH值为所述网关设备获取得到并拼接在第二URL中的HASH值；所述第一URL和所述第二URL的访问对象相同；

第二确定模块，用于在所述检测结果表征所述第一HASH值与所述第二HASH值不相同的情况下，确定所述第一WEB请求为异常访问请求。

9.一种网关设备，包括存储器、处理器以及存储在所述存储器中并可在所述处理器上运行的计算机程序，其特征在于，所述处理器执行所述计算机程序时实现如权利要求1至7任一项所述的异常访问检测方法。

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，所述程序指令当被处理器执行时使所述处理器执行如权利要求1至7任一项所述的异常访问检测方法。

异常访问检测方法、装置、网关设备及存储介质

技术领域

[0001] 本发明属于通信技术领域，尤其涉及一种异常访问检测方法、装置、网关设备及存储介质。

背景技术

[0002] 相关技术可以通过统一资源定位符(URL，Uniform Resource Locator)拼接来实现越权访问。越权访问可以访问用户权限之外的数据，甚至可以修改数据，因此对数据的安全性造成极大的威胁。目前，相关技术不能有效检测URL 拼接行为，只能通过复杂的权限校验来检测用户的越权访问。

发明内容

[0003] 有鉴于此，本发明实施例提供一种异常访问检测方法、装置、交换机及存储介质，以至少解决相关技术不能有效检测用户的URL拼接行为的问题。

[0004] 本发明实施例的技术方案是这样实现的：

[0005] 第一方面，本发明实施例提供了一种异常访问检测方法，应用于网关设备，该方法包括：

[0006] 接收第一全球广域网(WEB，World Wide Web)请求中的第一URL；

[0007] 确定所述第一URL是否携带第一哈希(HASH)值；

[0008] 在所述第一URL中携带所述第一HASH值的情况下，检测所述第一HASH 值与第二HASH值是否相同，得到检测结果；所述第二HASH值为所述网关设备获取得到并拼接在第二URL中的HASH值；所述第一URL和所述第二URL 的访问对象相同；

[0009] 在所述检测结果表征所述第一HASH值与所述第二HASH值不相同的情况下，确定所述第一WEB请求为异常访问请求。

[0010] 上述方案中，所述方法还包括：

[0011] 在所述第一URL未携带所述第一HASH值的情况下，确定所述第一URL 是否在设定的第一数据表中；当所述第一URL存储于所述第一数据表时，对应的所述第一WEB请求为正常访问请求；

[0012] 在所述第一URL不在所述设定的第一数据表中的情况下，确定所述第一 WEB请求为异常访问请求。

[0013] 上述方案中，在接收第一WEB请求之前，所述方法还包括：

[0014] 确定所述第一数据表；

[0015] 所述确定所述第一数据表，包括：

[0016] 接收关于所述访问对象的第二WEB请求；所述第二WEB请求中的第三 URL未携带HASH值；

[0017] 根据接收到的所述第二WEB请求，确定发起所述第二WEB请求的用户数量；

[0018] 在所述用户数量大于设定值的情况下，将所述第三URL写入所述第一数据表。

[0019] 上述方案中，所述根据接收到的所述第二WEB请求，确定发起所述第二 WEB请求的用户数量时，所述方法包括：

[0020] 在第一次接收到所述第二WEB请求时，将所述第三URL写入第二数据表中，并根据接收到的所述第二WEB请求实时更新所述第二数据表中所述第三 URL对应的用户数量。

[0021] 上述方案中，所述方法还包括：

[0022] 基于第四URL获取所述第二HASH值；

[0023] 将所述第二HASH值拼接在所述第四URL中，得到所述第二URL，以使终端设备根据所述第二URL访问所述访问对象；其中，

[0024] 所述第四URL为所述访问对象对应的资源地址。

[0025] 上述方案中，所述基于第四URL获取所述第二HASH值，包括：

[0026] 基于所述第四URL和设定信息获取所述第二HASH值；所述设定信息至少包括所述终端设备登录所述网关设备时对应的随机码。

[0027] 上述方案中，所述设定信息还包括以下任意一项或多项：

[0028] 所述终端设备登录所述网关设备时使用的用户信息；

[0029] 所述终端设备访问所述访问对象的WEB请求中携带的密钥。

[0030] 第二方面，本发明实施例提供了一种异常访问检测装置，该装置包括：

[0031] 接收模块，用于接收第一WEB请求中的第一URL；

[0032] 第一确定模块，用于确定所述第一URL是否携带第一HASH值；

[0033] 检测模块，用于在所述第一URL中携带所述第一HASH值的情况下，检测所述第一HASH值与第二HASH值是否相同，得到检测结果；所述第二HASH 值为所述网关设备获取得到并拼接在第二URL中的HASH值；所述第一URL 和所述第二URL的访问对象相同；

[0034] 第二确定模块，用于在所述检测结果表征所述第一HASH值与所述第二 HASH值不相同的情况下，确定所述第一WEB请求为异常访问请求。

[0035] 第三方面，本发明实施例提供了一种网关设备，包括处理器和存储器，所述处理器和存储器相互连接，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，执行本发明实施例第一方面提供的异常访问检测方法的步骤。

[0036] 第四方面，本发明实施例提供了一种计算机可读存储介质，包括：所述计算机可读存储介质存储有计算机程序。所述计算机程序被处理器执行时实现如本发明实施例第一方面提供的异常访问检测方法的步骤。

[0037] 本发明实施例通过接收第一WEB请求中的第一URL；确定第一URL是否携带第一HASH值；在第一URL携带第一HASH值的情况下，检测第一HASH 值与第二HASH值是否相同，得到检测结果；第二HASH值为网关设备获取得到并拼接在第二URL中的HASH值；第一URL和第二URL的访问对象相同；在检测结果表征第一HASH值与第二HASH值不相同的情况下，确定第一WEB 请求为异常访问请求。在本发明实施例中，网关设备能够通过检测第一HASH 值与第二HASH值是否相同来检测出WEB请求是否为URL拼接行为，若是，则拦截该WEB请求。本发明的网关设备能够保护所有经过网关设备代理的 WEB服务器的数据，避免非法访问、篡改和泄露WEB服务器中的数据。

附图说明

[0038] 图1是本发明实施例提供的一种网络拓扑结构的示意图；

[0039] 图2是本发明实施例提供的另一种异常访问检测方法的实现流程示意图；

[0040] 图3是本发明实施例提供的另一种异常访问检测方法的实现流程示意图；

[0041] 图4是本发明实施例提供的另一种异常访问检测方法的实现流程示意图；

[0042] 图5是本发明实施例提供的另一种异常访问检测方法的实现流程示意图；

[0043] 图6是本发明应用实施例提供的一种确定第二数据表的流程示意图；

[0044] 图7是本发明应用实施例提供的一种异常访问检测流程的示意图；

[0045] 图8是本发明实施例提供的一种异常访问检测装置的结构框图；

[0046] 图9是本发明实施例提供的网关设备的硬件结构示意图。

具体实施方式

[0047] 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。

[0048] 应当理解，当在本说明书和所附权利要求书中使用时，术语“包括”和“包含”指示所描述特征、整体、步骤、操作、元素和/或组件的存在，但并不排除一个或多个其它特征、整体、步骤、操作、元素、组件和/或其集合的存在或添加。

[0049] 需要说明的是，本发明实施例所记载的技术方案之间，在不冲突的情况下，可以任意组合。

[0050] 另外，在本发明实施例中，“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。

[0051] 为了说明本发明所述的技术方案，下面通过具体实施例来进行说明。

[0052] 参考图1，图1是本发明实施例提供的一种网络拓扑结构的示意图，该网络拓扑结构包括：终端设备、网关设备和全球广域网(WEB，World Wide Web) 服务器。

[0053] 其中，终端设备可以是手机、平板电脑、计算机等电子设备。

[0054] 在本发明实施例中，网关设备作为一个反向代理服务器来使用，反向代理服务器(网关设备)位于终端设备和WEB服务器之间，对于终端设备而言，反向代理服务器(网关设备)就相当于WEB服务器，终端设备直接访问反向代理服务器(网关设备)就可以获得WEB服务器的资源。

[0055] 反向代理服务器的反向代理过程为：终端设备发往WEB服务器的WEB请求都会先发送到反向代理服务器，反向代理服务器接收到终端设备的WEB请求后，将WEB请求转发至WEB服务器。WEB服务器接收到WEB请求后，响应WEB请求，发送WEB响应给反向代理服务器。反向代理服务器接收WEB 响应，改写WEB响应中的URL地址，并将改写后的WEB响应发送给终端设备。其中，反向代理服务器需要改写WEB响应中的URL地址，例如，企业某个内部网络地址为1.1.1.1，在反向代理过程中，反向代理服务器得到的WEB 响应中的超链接地址为1.1.1.1，而终端设备是无法点击访问该内部网络地址的，反向代理服务器只有将该内部网络地址改写为WWW.XX.COM的格式，终端设备才能点击进行访问。因此，反向代理服务器需要改写WEB

响应中的URL地址,改写成终端设备能够访问的URL地址。

[0056] URL地址除了携带有访问对象的资源地址外,还携带有一些参数,例如,用户信息、主机名、端口号等参数。这些参数和资源地址一起拼接成了一个完整的URL地址,移动终端通过该URL地址,即可访问访问对象。由于这些参数并不隐秘,网络黑客窃取到这些参数并不困难,网络黑客可以通过URL拼接来获得完整的URL地址,从而实现越权访问。因此,相关技术可以通过URL 拼接来非法访问、篡改和泄露WEB服务器中的数据。然而,相关技术无法识别网络黑客的URL拼接行为,只能通过复杂的权限校验来检测网络黑客的越权访问。

[0057] 在本发明实施例中,网关设备在改写WEB响应中的URL地址时,获取该 URL地址的HASH值,并将HASH值拼接在该URL地址中。HASH值是指通过一定的哈希算法对文件内容进行加密运算得到的一组二进制值,不同的文件内容得到的HASH值不同,因此HASH值可用于文件内容唯一性判别。其中,哈希算法可以是信息摘要算法(MD5,Message Digest Algorithm 5)或安全散列算法(SHA,Secure Hash Algorithm)。然后网关设备将携带有改写后的URL地址的WEB响应发送给终端设备,终端设备接收到WEB响应后,如果终端设备要访问该URL地址对应的访问对象,终端设备需要通过携带有该HASH值的URL地址才能访问该访问对象。此外,将网关设备作为反向代理服务器,对外表现为一个WEB服务器,不同之处在于,网关设备没有保存任何网页的真实数据,所有网页的真实数据都保存在WEB服务器上。因此对网关设备的攻击并不会使得网页信息遭到破坏,这样就增强了WEB服务器的安全性。其次,通过网关设备来中转终端设备的WEB请求,可以降低网络和WEB服务器的负载,提高访问效率。

[0058] 在实际应用中,上述网关设备可以为零信任网关设备,零信任是一种网络架构中,零信任网络架构的核心思想是“从不信任,始终验证”,即企业不应该信任网络内部和外部的任何人、设备和系统,应在授权前对任何试图接入企业系统的人、设备和系统进行验证。这里,零信任网关设备除了用于验证URL 地址的HASH值外,还用于对用户、设备和系统进行验证。零信任网关接收终端设备发送的WEB请求,对WEB请求对应的终端设备和用户进行验证,只有验证通过的终端设备和用户,并且需要具备足够的权限才能访问WEB服务器。通过零信任网关设备,可以提升WEB服务器中数据的安全性,避免非法访问、篡改和泄露WEB服务器中的数据。

[0059] 图2是本发明实施例提供的一种异常访问检测方法的实现流程示意图,该方法执行主体为图1中的网关设备。参考图2,异常访问检测方法包括:

[0060] S101,接收第一WEB请求中的第一URL。

[0061] 终端设备发送给WEB服务器的WEB请求都会发送到网关设备,网关设备接收终端设备发送的WEB请求,获取第一WEB请求中的第一URL。在实际应用中,一个WEB请求由请求行(request line)、请求头部(header)、空行和请求数据四个部分组成。其中,URL位于请求行中。

[0062] 由于第一WEB请求需要经过网关设备,因此第一WEB请求中的所有内容对于网关来说都是明文,网关设备解析终端设备发送的第一WEB请求,获取第一WEB请求中的第一URL,第一URL指第一WEB请求对应的访问对象的资源地址,根据该资源地址可以在访问对象对应的WEB服务器上定位到该访问对象所在的资源位置。

[0063] S102,确定所述第一URL是否携带第一HASH值。

[0064] 这里,第一HASH值为携带在第一URL中的HASH值。在本发明实施例中,可以设定第

一HASH值在第一URL中的位置，如果第一URL携带第一 HASH值，但是携带的第一HASH值在第一URL中的位置与设定位置不吻合，也会确定为第一URL未携带第一HASH值。例如，假设第一URL为“https://www.xxxxx.com/6264858.html”，如果第一HASH值在第一URL中的设定位置为com和html的中间，第一HASH值为6264858，则认为上述第一 URL携带第一HASH值。只有第一HASH值在第一URL中的位置正确，才确定第一URL携带第一HASH值。

[0065] S103，在所述第一URL中携带所述第一HASH值的情况下，检测所述第一HASH值与第二HASH值是否相同，得到检测结果；所述第二HASH值为所述网关设备获取得到并拼接在第二URL中的HASH值；所述第一URL和所述第二URL的访问对象相同。

[0066] 如果第一URL中携带有第一HASH值，检测第一HASH值与第二HASH 值是否相同，得到检测结果。其中，第二HASH值为第二URL中的HASH值，第一URL和所述第二URL的访问对象相同，也就是说第一URL和第二URL 除了HASH值或者HASH值在URL中的位置可能不同，其余参数都相同。

[0067] 第二HASH值为所述网关设备获取得到并拼接在第二URL中的HASH值，对于第二URL的生成方法，参考图3，在一实施例中，异常访问检测方法还包括：

[0068] S301，基于第四URL获取所述第二HASH值。

[0069] 在实际应用中，网关设备可以根据哈希运算消息认证码(HMAC， Hash-based Message Authentication Code)算法、信息摘要算法(MD5，Message Digest Algorithm 5)或安全散列算法(SHA，Secure Hash Algorithm)来获取第四URL的第二HASH值。这里，第四URL为所述访问对象对应的资源地址，也就是未携带HASH值的URL地址。

[0070] 进一步的，所述基于第四URL获取所述第二HASH值，包括：

[0071] 基于所述第四URL和设定信息获取所述第二HASH值；所述设定信息至少包括所述终端设备登录所述网关设备时对应的随机码。

[0072] 终端设备需要登录网关设备后，才能发送WEB请求至网关设备。在本发明实施例中，终端设备在登录网关设备时，网关设备会发送一个随机生成的随机码给终端设备，终端设备通过随机码验证之后，才能成功登录网关设备。

[0073] 网关设备可以基于该随机码和第四URL获取第二HASH值，这样由于终端设备每次登录网关设备时，网关设备生成的随机码都不同，那么网关设备每次获取得到的第二HASH值都不同，这样增加了第二HASH值被破解的难度，提升了WEB服务器中数据的安全性。

[0074] 进一步的，所述设定信息还包括以下任意一项或多项：

[0075] 所述终端设备登录所述网关设备时使用的用户信息；

[0076] 所述终端设备访问所述访问对象的WEB请求中携带的密钥。

[0077] 终端设备登录网关设备时除了需要随机码，还需要能够表征用户身份的用户信息，例如身份证号、用户名称等用户信息。

[0078] 终端设备访问所述访问对象的WEB请求中携带的密钥，这里，密钥可以是终端设备登录网关设备的登录密码，也可以是终端设备登录WEB服务器的登录密码。

[0079] S302，将所述第二HASH值拼接在所述第四URL中，得到所述第二URL，以使终端设备根据所述第二URL访问所述访问对象；其中，所述第四URL为所述访问对象对应的资源地址。

[0080] 网关设备可以通过字符串拼接将第二HASH值拼接在第四URL中，例如，假设第四URL为“https://www.xxxxx.com.html”，第二哈希HASH值为6264858，则通过字符串拼接，得

到携带有第二HASH值的第二URL，第二URL为“https://www.xxxxx.com/6264858.html”。

[0081] 网关设备将携带有第二HASH值的第二URL发送给终端设备，以使终端设备根据所述第二URL访问所述访问对象。也就是说，终端设备只有通过携带有第二HSAH值的第二URL才能访问所述访问对象，终端设备无法再根据第四URL访问所述访问对象。这样，由于除了终端设备知道第二HASH值，其他终端无法知道第二HASH值，也就无法拼接出第二URL，因此无法做出越权访问行为。

[0082] 在实际应用中，网关设备可以预先将第二HASH值存储在网关设备中，在检测所述第一HASH值与第二HASH值是否相同时，读取出第二HASH值。

[0083] S104，在所述检测结果表征所述第一HASH值与所述第二HASH值不相同的情况下，确定所述第一WEB请求为异常访问请求。

[0084] 如果检测结果表征第一HASH值与第二HASH值不相同，说明第一WEB 请求不是终端设备发出的，第一WEB请求中的第一URL是其他终端设备的 URL拼接行为产生的，因此确定第一WEB请求为异常访问请求。

[0085] 在实际应用中，对于异常访问请求，网关设备可以进行拦截，并向终端设备发送预警信息。

[0086] 本发明实施例通过接收第一WEB请求中的第一URL；确定第一URL是否携带第一HASH值；在第一URL中携带第一HASH值的情况下，检测第一HASH 值与第二HASH值是否相同，得到检测结果；第二HASH值为网关设备获取得到并拼接在第二URL中的HASH值；第一URL和第二URL的访问对象相同；在检测结果表征第一HASH值与第二HASH值不相同的情况下，确定第一WEB 请求为异常访问请求。在本发明实施例中，网关设备能够通过检测第一HASH 值与第二HASH值是否相同来检测出URL拼接行为，拦截URL拼接行为造成的越权访问。网关设备能够保护所有经过网关设备代理的WEB服务器，避免非法访问、篡改和泄露WEB服务器中的数据。

[0087] 进一步的，参考图4，在上述实施例中，异常访问检测方法还包括：

[0088] S401，在所述第一URL未携带所述第一HASH值的情况下，确定所述第一URL是否在设定的第一数据表中；当所述第一URL存储于所述第一数据表时，对应的所述第一WEB请求为正常访问请求。

[0089] 在上述实施例中，所有URL中都携带有HASH值，只有HASH值正确，访问才是正常的。然而在有些情况下，某些WEB请求中的URL并未携带HASH 值，但是这些访问也是正常的。例如，部分企业办公系统(OA，Office Automation) 的首页，用户从使用角度上来说习惯于直接输入首页地址进行访问，而且这些首页地址并不需要进行数据保护，任何用户都能访问。

[0090] 在本发明实施例中，将所有正常访问请求对应的URL写入设定的第一数据库中，在第一URL未携带第一HASH值的情况下，确定第一URL是否在设定的第一数据表中，如果第一URL设定的第一数据表中，说明第一URL对应的 WEB请求为正常访问请求。

[0091] 本发明实施例需要预先确定第一数据表，才能根据第一数据表对WEB请求进行异常检测。

[0092] 参考图5，在一实施例中，在接收第一WEB请求之前，异常访问检测方法还包括：

[0093] 确定所述第一数据表。

[0094] 所述确定所述第一数据表，包括：

[0095] S501,接收关于所述访问对象的第二WEB请求;所述第二WEB请求中的第三URL未携带HASH值。

[0096] 在本发明实施例中,第三URL中未携带HASH值。

[0097] S502,根据接收到的所述第二WEB请求,确定发起所述第二WEB请求的用户数量。

[0098] 第二WEB请求中携带有用户身份信息,每接收到一个第二WEB请求,就记录其中的用户信息。确定发起第二WEB请求的用户数量,对于同一个用户的多次访问,将对应的用户数量记录为1。例如,A用户发起过3次第二WEB 请求,B用户发起过2次WEB请求,则发起第二WEB请求的用户数量为2。

[0099] S503,在所述用户数量大于设定值的情况下,将所述第三URL写入所述第一数据表。

[0100] 如果发起第二WEB请求的用户数量大于设定值,说明发起第二WEB请求的人数较多,可以认为第二WEB请求是一个正常的访问请求,将该第二WEB 请求中的第三URL写入第一数据表中,第一数据表中的URL对应的WEB请求为正常访问请求。

[0101] 进一步的,所述根据接收到的所述第二WEB请求,确定发起所述第二WEB 请求的用户数量时,所述方法包括:

[0102] 在第一次接收到所述第二WEB请求时,将所述第三URL写入第二数据表中,并根据接收到的所述第二WEB请求实时更新所述第二数据表中所述第三 URL对应的用户数量。

[0103] 在第一次接收到所述第二WEB请求时,将第三URL写入第二数据表中,并在第二数据表中记录第三URL对应的用户信息,第二数据表中有多少不同的用户信息,就对应多少用户数量。网关设备根据接收到的第二WEB请求实时更新第二数据表中第三URL对应的用户数量,在第三URL对应的用户数量大于设定值的情况下,将所述第三URL写入第一数据表。

[0104] S402,在所述第一URL不在所述设定的第一数据表中的情况下,确定所述第一WEB请求为异常访问请求。

[0105] 如果第一URL不在设定的第一数据表中,确定第一URL对应的第一WEB 请求为异常访问请求。

[0106] 对于那些不在设定的第一数据表中的URL,由于访问人数较少,有可能是黑客访问行为,将这些URL对应的WEB请求确定为异常访问请求。在实际应用中,对于那些没有写入第一数据表中的URL,用户可以登录网关设备申请将URL写入第一数据表,管理员可以登录网关设备对用户的申请进行同意或拒绝。

[0107] 参考图6,图6是本发明应用实施例提供的一种确定第二数据表的流程示意图,所述确定第二数据表的流程包括:

[0108] S601,获取WEB请求中的URL。

[0109] S602,判断所述URL是否携带HASH值。

[0110] 如果携带HASH值,则结束流程。如果未携带HASH值,则执行步骤S603。

[0111] S603,判断所述URL和对应的用户信息是否存储在数据库中。

[0112] 这里,数据库指的是上述实施例中的第二数据表。

[0113] 如果所述URL和对应的用户信息存储在了数据库中了,则结束流程。如果所述URL和对应的用户信息没有存储在了数据库中,则执行步骤S604。

[0114] S604,在数据库中写入所述URL和对应的用户信息。

[0115] 参考图7,图7是本发明应用实施例提供的一种异常访问检测流程的示意图,所述异常访问检测流程包括:

[0116] S701,网关设备接收WEB请求。

[0117] S702,判断所述WEB请求中的URL是否携带HASH值。

[0118] 如果携带HASH值,则执行S703。如果未携带HASH值,则执行S706。

[0119] S703,判断所述HASH值是否正确。

[0120] 如果HASH值正确,则执行S704。如果HASH值错误,则执行S705。

[0121] S704,确定所述WEB请求为正常访问请求。

[0122] S705,确定所述WEB请求为异常访问请求。

[0123] S706,判断所述WEB请求中的URL是否在白名单中。

[0124] 这里,所述白名单为上述实施例中的设定的第一数据表。

[0125] 如果URL在白名单中,则执行S704。如果URL不在白名单中,则执行 S705。

[0126] 本发明应用实施例中,网关设备通过接受终端设备发送的WEB请求,获取WEB请求中的URL,判断所述URL中的HASH值是否正确,在HASH值正确的情况下,确定WEB请求为正常访问请求,反之确定为异常访问请求。对于未携带HASH值的URL,通过判断URL是否在白名单中,对于在白名单中的URL,确定WEB请求为正常访问请求,反之确定为异常访问请求。本发明实施例可以检测出URL拼接行为,拦截URL拼接行为造成的越权访问。网关设备能够保护所有经过网关设备代理的WEB服务器,避免非法访问、篡改和泄露WEB服务器中的数据。

[0127] 应理解,上述实施例中各步骤的序号的大小并不意味着执行顺序的先后,各过程的执行顺序应以其功能和内在逻辑确定,而不应对本发明实施例的实施过程构成任何限定。

[0128] 参考图8,图8是本发明实施例提供的一种异常访问检测装置的示意图,如图8所示,该装置包括:接收模块、第一确定模块、检测模块和第二确定模块。

[0129] 接收模块,用于接收第一全球广域网WEB请求中的第一统一资源定位符 URL;

[0130] 第一确定模块,用于确定所述第一URL是否携带第一哈希HASH值;

[0131] 检测模块,用于在所述第一URL中携带所述第一HASH值的情况下,检测所述第一HASH值与第二HASH值是否相同,得到检测结果;所述第二HASH 值为所述网关设备获取得到并拼接在第二URL中的HASH值;所述第一URL 和所述第二URL的访问对象相同;

[0132] 第二确定模块,用于在所述检测结果表征所述第一HASH值与所述第二 HASH值不相同的情况下,确定所述第一WEB请求为异常访问请求。

[0133] 所述装置还包括:

[0134] 第三确定模块,用于在所述第一URL未携带所述第一HASH值的情况下,确定所述第一URL是否在设定的第一数据表中;当所述第一URL存储于所述第一数据表时,对应的所述第一WEB请求为正常访问请求;

[0135] 第四确定模块,用于在所述第一URL不在所述设定的第一数据表中的情况下,确定所述第一WEB请求为异常访问请求。

[0136] 在接收第一WEB请求之前,所述装置还包括:

[0137] 第五确定模块,用于确定所述第一数据表;

[0138] 所述装置还包括:

[0139] 第二接收模块，用于接收关于所述访问对象的第二WEB请求；所述第二 WEB请求中的第三URL未携带HASH值；

[0140] 第六确定模块，用于根据接收到的所述第二WEB请求，确定发起所述第二WEB请求的用户数量；

[0141] 写入模块，用于在所述用户数量大于设定值的情况下，将所述第三URL写入所述第一数据表。

[0142] 所述写入模块具体用于：在第一次接收到所述第二WEB请求时，将所述第三URL写入第二数据表中，并根据接收到的所述第二WEB请求实时更新所述第二数据表中所述第三URL对应的用户数量。

[0143] 所述装置还包括：

[0144] 获取模块，用于基于第四URL获取所述第二HASH值；

[0145] 拼接模块，用于将所述第二HASH值拼接在所述第四URL中，得到所述第二URL，以使终端设备根据所述第二URL访问所述访问对象；其中，

[0146] 所述第四URL为所述访问对象对应的资源地址。

[0147] 所述获取模块具体用于：基于所述第四URL和设定信息获取所述第二 HASH值；所述设定信息至少包括所述终端设备登录所述网关设备时对应的随机码。

[0148] 所述设定信息还包括以下任意一项或多项：

[0149] 所述终端设备登录所述网关设备时使用的用户信息；

[0150] 所述终端设备访问所述访问对象的WEB请求中携带的密钥。

[0151] 需要说明的是：上述实施例提供的异常访问检测装置在进行异常访问检测时，仅以上述各模块的划分进行举例说明，实际应用中，可以根据需要而将上述处理分配由不同的模块完成，即将装置的内部结构划分成不同的模块，以完成以上描述的全部或者部分处理。另外，上述实施例提供的异常访问检测装置与异常访问检测方法实施例属于同一构思，其具体实现过程详见方法实施例，这里不再赘述。

[0152] 图9是本发明一实施例提供的网关设备的示意图。所述网关设备包括：手机、平板、服务器等。如图9所示，该实施例的网关设备包括：处理器、存储器以及存储在所述存储器中并可在所述处理器上运行的计算机程序。所述处理器执行所述计算机程序时实现上述各个方法实施例中的步骤，例如图1所示的步骤101至104。或者，所述处理器执行所述计算机程序时实现上述各装置实施例中各模块的功能，例如图8所示接收模块、第一确定模块、检测模块和第二确定模块的功能。

[0153] 示例性的，所述计算机程序可以被分割成一个或多个模块，所述一个或者多个模块被存储在所述存储器中，并由所述处理器执行，以完成本发明。所述一个或多个模块可以是能够完成特定功能的一系列计算机程序指令段，该指令段用于描述所述计算机程序在所述网关设备中的执行过程。

[0154] 所述网关设备可包括，但不仅限于，处理器、存储器。本领域技术人员可以理解，图9仅仅是网关设备的示例，并不构成对网关设备的限定，可以包括比图示更多或更少的部件，或者组合某些部件，或者不同的部件，例如所述网关设备还可以包括输入输出设备、网络接入设备、总线等。

[0155] 所称处理器可以是中央处理单元(Central Processing Unit，CPU)，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。

[0156] 所述存储器可以是所述网关设备的内部存储单元,例如网关设备的硬盘或内存。所述存储器也可以是所述网关设备的外部存储设备,例如所述网关设备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,所述存储器还可以既包括所述网关设备的内部存储单元也包括外部存储设备。所述存储器用于存储所述计算机程序以及所述网关设备所需的其他程序和数据。所述存储器还可以用于暂时地存储已经输出或者将要输出的数据。

[0157] 所属领域的技术人员可以清楚地了解到,为了描述的方便和简洁,仅以上述各功能单元、模块的划分进行举例说明,实际应用中,可以根据需要而将上述功能分配由不同的功能单元、模块完成,即将所述装置的内部结构划分成不同的功能单元或模块,以完成以上描述的全部或者部分功能。实施例中的各功能单元、模块可以集成在一个处理单元中,也可以是各个单元单独物理存在,也可以两个或两个以上单元集成在一个单元中,上述集成的单元既可以采用硬件的形式实现,也可以采用软件功能单元的形式实现。另外,各功能单元、模块的具体名称也只是为了便于相互区分,并不用于限制本申请的保护范围。上述系统中单元、模块的具体工作过程,可以参考前述方法实施例中的对应过程,在此不再赘述。

[0158] 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或记载的部分,可以参见其它实施例的相关描述。

[0159] 本领域普通技术人员可以意识到,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、或者计算机软件和电子硬件的结合来实现。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。专业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发明的范围。

[0160] 在本发明所提供的实施例中,应该理解到,所揭露的装置/网关设备和方法,可以通过其它的方式实现。例如,以上所描述的装置/网关设备实施例仅仅是示意性的,例如,所述模块或单元的划分,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,例如多个单元或组件可以结合或者可以集成到另一个系统,或一些特征可以忽略,或不执行。另一点,所显示或讨论的相互之间的耦合或直接耦合或通讯连接可以是通过一些接口,装置或单元的间接耦合或通讯连接,可以是电性,机械或其它的形式。

[0161] 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单元来实现本实施例方案的目的。

[0162] 另外,在本发明各个实施例中的各功能单元可以集成在一个处理单元中,也可以是各个单元单独物理存在,也可以两个或两个以上单元集成在一个单元中。上述集成的单元既可以采用硬件的形式实现,也可以采用软件功能单元的形式实现。

[0163] 所述集成的模块/单元如果以软件功能单元的形式实现并作为独立的产品销售或使用时，可以存储在一个计算机可读取存储介质中。基于这样的理解，本发明实现上述实施例方法中的全部或部分流程，也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计算机可读存储介质中，该计算机程序在被处理器执行时，可实现上述各个方法实施例的步骤。其中，所述计算机程序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(Read-Only Memory，ROM)、随机存取存储器(Random Access Memory，RAM)、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。

[0164] 以上所述实施例仅用以说明本发明的技术方案，而非对其限制；尽管参照前述实施例对本发明进行了详细的说明，本领域的普通技术人员应当理解：其依然可以对前述各实施例所记载的技术方案进行修改，或者对其中部分技术特征进行等同替换；而这些修改或者替换，并不使相应技术方案的本质脱离本发明各实施例技术方案的精神和范围，均应包含在本发明的保护范围之内。

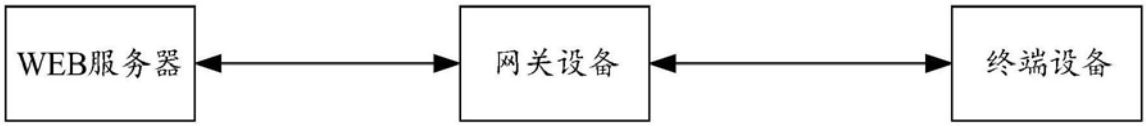

WEB服务器
网关设备
终端设备

图1

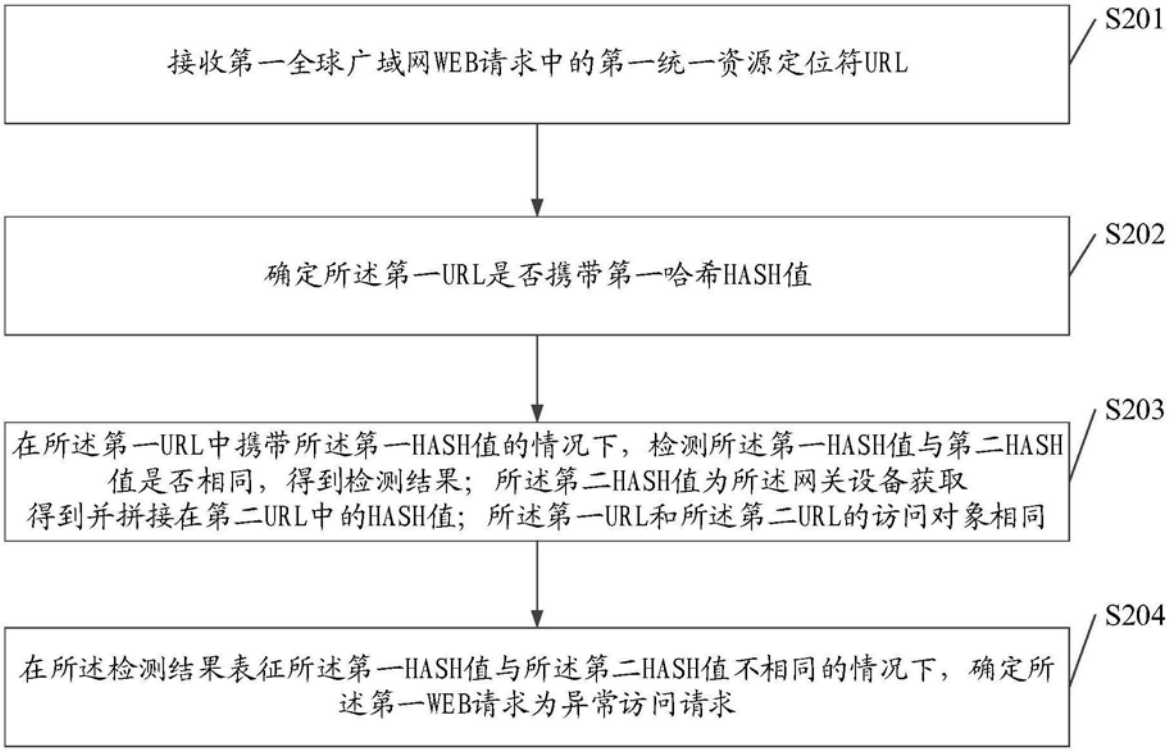

接收第一全球广域网WEB请求中的第一统一资源定位符URL
S201
确定所述第一URL是否携带第一哈希HASH值
S202
在所述第一URL中携带所述第一HASH值的情况下，检测所述第一HASH值与第二HASH值是否相同，得到检测结果；所述第二HASH值为所述网关设备获取得到并拼接在第二URL中的HASH值；所述第一URL和所述第二URL的访问对象相同
S203
在所述检测结果表征所述第一HASH值与所述第二HASH值不相同的情况下，确定所述第一WEB请求为异常访问请求
S204

图2

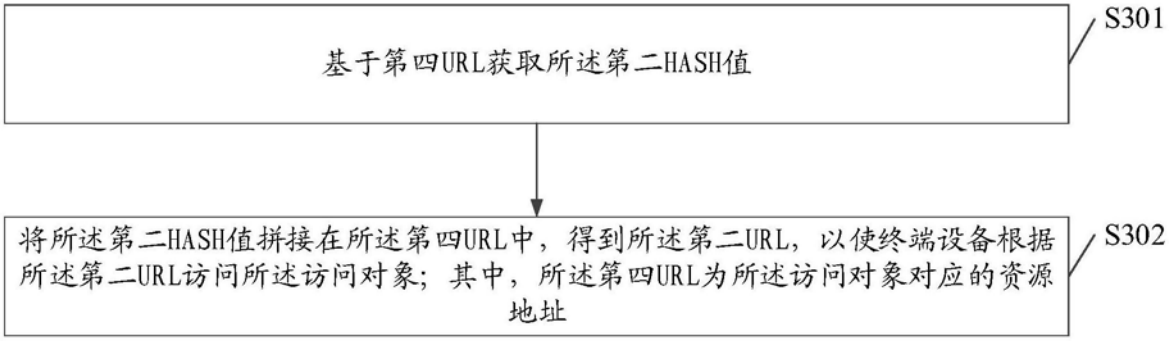

基于第四URL获取所述第二HASH值
S301
将所述第二HASH值拼接在所述第四URL中，得到所述第二URL，以使终端设备根据所述第二URL访问所述访问对象；其中，所述第四URL为所述访问对象对应的资源地址
S302

图3

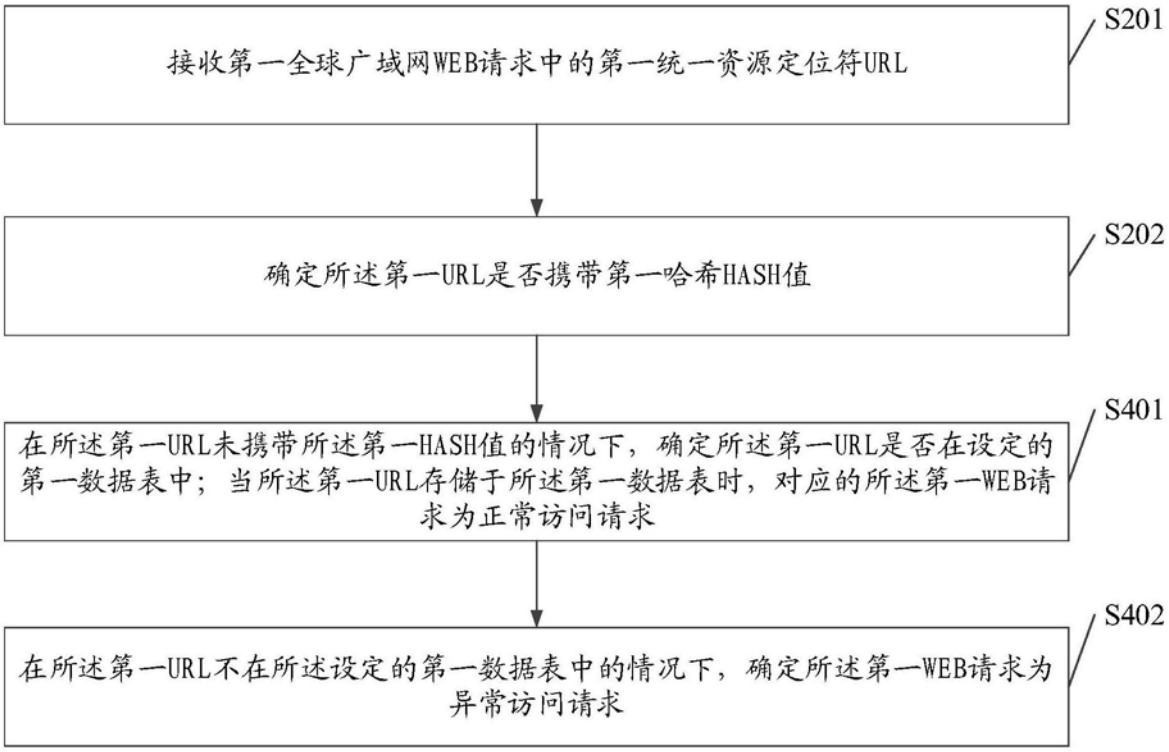

S201
接收第一全球广域网WEB请求中的第一统一资源定位符URL
S202
确定所述第一URL是否携带第一哈希HASH值
S401
在所述第一URL未携带所述第一HASH值的情况下，确定所述第一URL是否在设定的第一数据表中；当所述第一URL存储于所述第一数据表时，对应的所述第一WEB请求为正常访问请求
S402
在所述第一URL不在所述设定的第一数据表中的情况下，确定所述第一WEB请求为异常访问请求

图4

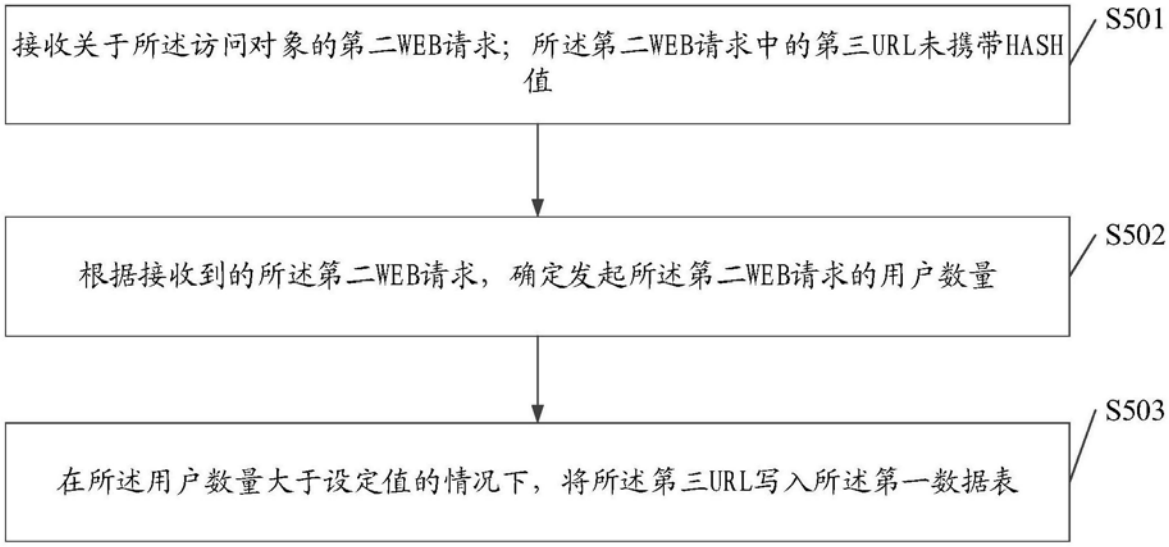

S501
接收关于所述访问对象的第二WEB请求；所述第二WEB请求中的第三URL未携带HASH值
S502
根据接收到的所述第二WEB请求，确定发起所述第二WEB请求的用户数量
S503
在所述用户数量大于设定值的情况下，将所述第三URL写入所述第一数据表

图5

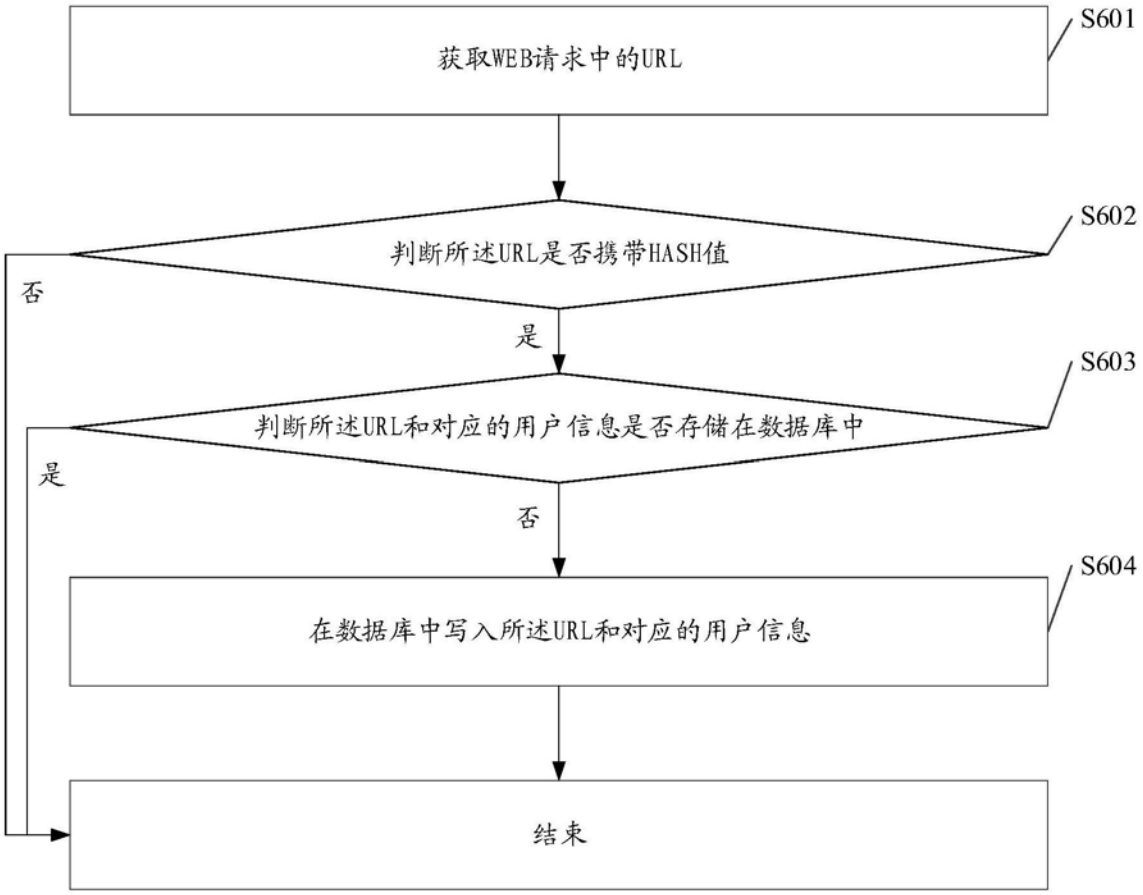

S601
获取WEB请求中的URL
S602
判断所述URL是否携带HASH值
否
是
S603
判断所述URL和对应的用户信息是否存储在数据库中
是
否
S604
在数据库中写入所述URL和对应的用户信息
结束

图6

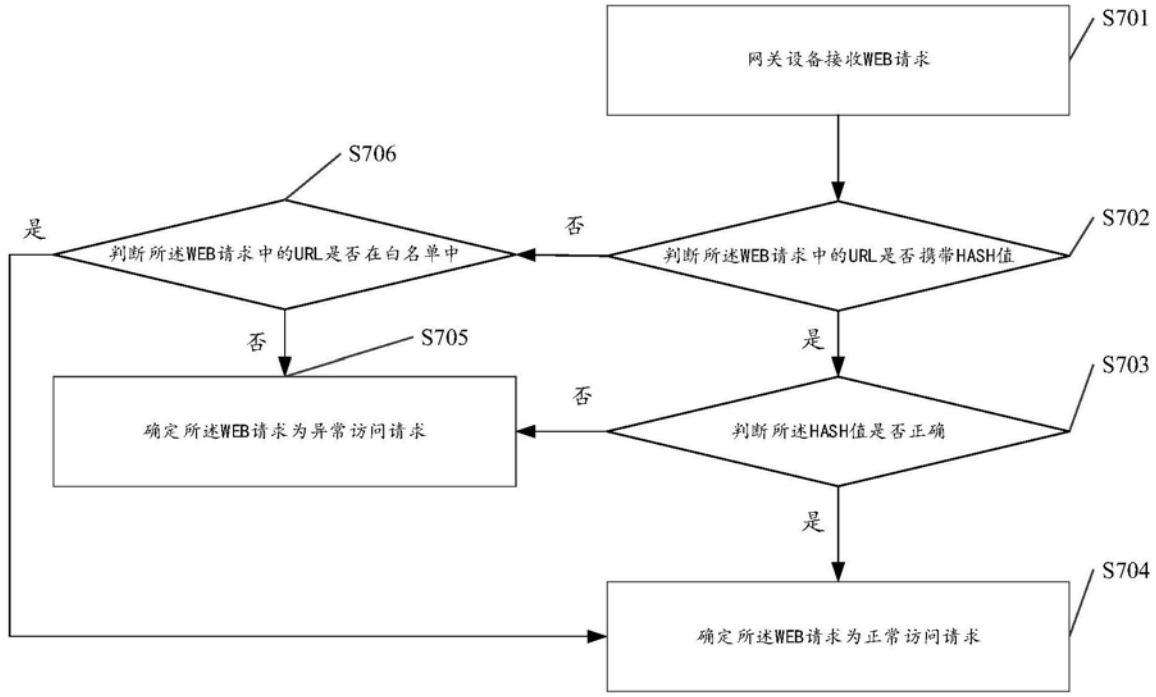

网关设备接收WEB请求
S701
判断所述WEB请求中的URL是否携带HASH值
S702
否
判断所述WEB请求中的URL是否在白名单中
S706
是
是
判断所述HASH值是否正确
S703
否
确定所述WEB请求为异常访问请求
S705
否
是
确定所述WEB请求为正常访问请求
S704

图7

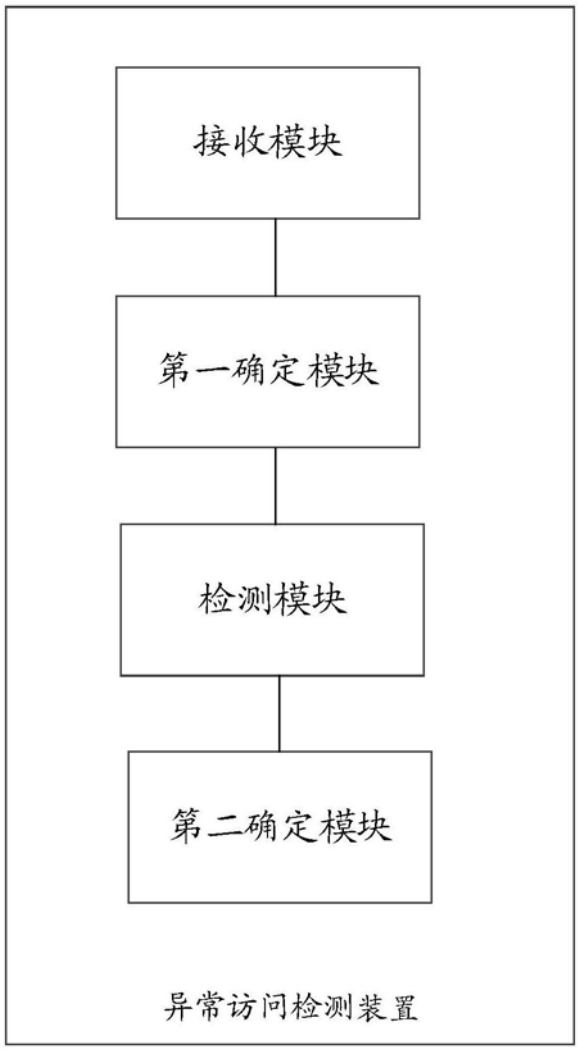


图8

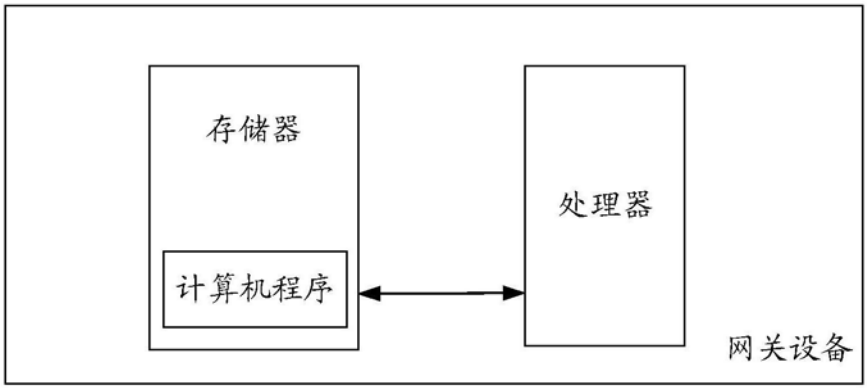


图9