(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2018 年 9 月 20 日 (20.09.2018)

WIPO | PCT

(10) 国际公布号
WO 2018/166365 A1

(51) 国际专利分类号:
H04L 12/24 (2006.01)

(21) 国际申请号: PCT/CN2018/077965

(22) 国际申请日: 2018 年 3 月 5 日 (05.03.2018)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201710153803.4 2017年3月15日 (15.03.2017) CN

(71) 申请人: 阿里巴巴集团控股有限公司 (ALIBABA GROUP HOLDING LIMITED) [—/CN]; 开曼群岛大开曼资本大厦一座四层 847 号邮箱, Grand Cayman (KY)。

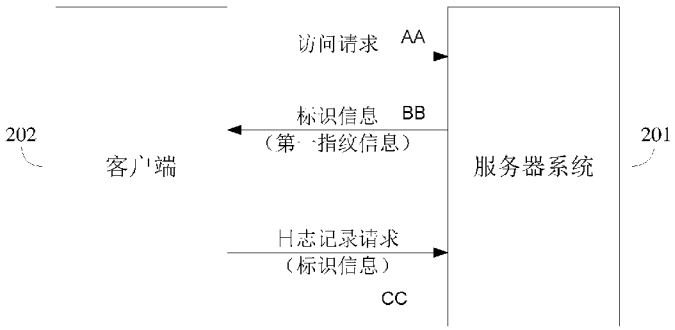
(72) 发明人: 吴鸣刚 (WU, Minggang); 中国浙江省杭州市余杭区文一西路969号3号楼5楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。 乔平 (QIAO, Ping); 中国浙江省杭州市余杭区文一西路969号3号楼5楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。

(74) 代理人: 北京三友知识产权代理有限公司 (BEIJING SANYOU INTELLECTUAL PROPERTY AGENCY LTD.); 中国北京市金融街 35 号国际企业大厦 A 座 16 层, Beijing 100033 (CN)。

(81) 指定国 (除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL,

(54) **Title:** METHOD AND DEVICE FOR RECORDING WEBSITE ACCESS LOG

(54) **发明名称:** 一种记录网站访问日志的方法和装置



201 Server system
202 Client
AA Access request
BB Identification information (first fingerprint information)
CC Log recording request (identification information)

图 2

(57) **Abstract:** Disclosed in embodiments of the present application is a method for recording a website access log. The method comprises: receiving an access request sent by a client; generating first fingerprint information using related information of the access request by means of a fingerprint algorithm; sending identification information carrying the first fingerprint information to the client; receiving a log recording request, the log recording request being used for requesting to record an access behavior; generating second fingerprint information using related information of the access behavior by means of the fingerprint algorithm; if the log recording request meets a recording condition, recording the access behavior in a website access log; and if the log recording request does not meet the recording condition, refusing to record the access behavior in a website access log, wherein the recording condition is that the log recording request carries the identification information and the first fingerprint information is identical to the second fingerprint information. In addition, also disclosed in the embodiments of the present application are a device for recording a website access log and a system.

WO 2018/166365 A1

[见续页]

PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(84) 指定国(除另有指明，要求每一种可提供的地区保护)：ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布：

— 包括国际检索报告(条约第21条(3))。

(57) 摘要：本申请实施例公开了一种记录网站访问日志的方法。该方法包括：接收客户端发送的访问请求；通过指纹算法将所述访问请求的相关信息生成第一指纹信息；向所述客户端发送携带有所述第一指纹信息的标识信息；接收日志记录请求，所述日志记录请求用于请求记录访问行为；通过所述指纹算法将所述访问行为的相关信息生成第二指纹信息；若所述日志记录请求满足记录条件，将所述访问行为记录到网站访问日志；若所述日志记录请求不满足记录条件，拒绝将所述访问行为记录到网站访问日志；其中，所述记录条件为：所述日志记录请求中携带有所述标识信息且所述第一指纹信息与所述第二指纹信息相同。此外，本申请实施例还公开了一种记录网站访问日志的装置和系统。

一种记录网站访问日志的方法和装置

本申请要求2017年03月15日递交的申请号为201710153803.4、发明名称为“一种记录网站访问日志的方法和装置”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

本申请涉及网络技术领域，特别涉及一种记录网站访问日志的方法和装置。

背景技术

在用户访问网站的过程中，用户的访问行为可以被记录到网站访问日志，从而用于实现用户行为分析等功能。具体地，用户向网站的服务器发送访问请求，网站的服务器向用户返回用户所请求的网站信息，并且，在发送访问请求之后，用户会向网站的服务器发送与该访问请求对应的日志记录请求，网站的服务器基于该日志记录请求将用户在该访问请求下产生的访问行为记录到网站访问日志。

发明人经过研究发现，有些用户会在实际上没有对网站信息进行访问的情况下伪造与访问请求对应的日志记录请求并向网站的服务器发送，以期网站的服务器将实际上没有真实发生过的用户访问行为记录到网站访问日志，从而达到刷网页访问流量等恶意行为。但是，网站的服务器在接收到用户的日志记录请求时往往无法准确地区分用户请求记录的用户访问行为是否真实发生过，因此，网站的服务器难以避免地会将没有真实发生过的用户访问行为记录到网站访问日志。

发明内容

本申请实施例所要解决的技术问题是，提供一种记录网站访问记录的方法和装置，以使得网站的服务器在接收到用户的日志记录请求时能够准确地区分用户请求记录的用户访问行为是否真实发生过，从而避免网站的服务器将没有真实发生过的用户访问行为记录到网站访问日志。

第一方面，本申请实施例提供了一种记录网站访问日志的系统，包括客户端和服务器系统；

所述服务器系统，用于接收所述客户端发送的访问请求并获取所述访问请求的相关信息，通过指纹算法将所述访问请求的相关信息生成第一指纹信息，向所述客户端发送

携带有所述第一指纹信息的标识信息，接收用于请求对访问行为进行记录的日志记录请求并获取所述访问行为的相关信息，通过所述指纹算法将所述访问行为的相关信息生成第二指纹信息，若所述日志记录满足记录条件则按照所述日志记录请求将所述访问行为记录到网站访问日志，若所述日志记录不满足记录条件则拒绝按照所述日志记录请求将所述访问行为记录到网站访问日志；

所述客户端，用于向所述服务器系统发送访问请求并接收所述服务器系统针对所述访问请求返回的所述标识信息，将所述标识信息携带在所述日志访问请求中向所述服务器系统发送；

其中，所述记录条件为：所述日志记录请求中携带有所述标识信息且所述第一指纹信息与所述第二指纹信息相同。

第二方面，本申请实施例提供了一种记录网站访问日志的方法，应用于服务器系统，包括：

接收客户端发送的访问请求并获取所述访问请求的相关信息；

通过指纹算法，将所述访问请求的相关信息生成第一指纹信息；

向所述客户端发送携带有所述第一指纹信息的标识信息；

接收日志记录请求并获取访问行为的相关信息，所述日志记录请求用于请求对所述访问行为进行记录；

通过所述指纹算法，将所述访问行为的相关信息生成第二指纹信息；

若所述日志记录请求满足记录条件，按照所述日志记录请求将所述访问行为记录到网站访问日志；

若所述日志记录请求不满足记录条件，拒绝按照所述日志记录请求将所述访问行为记录到网站访问日志；

其中，所述记录条件为：所述日志记录请求中携带有所述标识信息且所述第一指纹信息与所述第二指纹信息相同。

第三方面，本申请实施例提供了一种记录网站访问日志的方法，应用于客户端，包括：

向服务器系统发送访问请求，以便所述服务器系统获取所述访问请求的相关信息并通过指纹算法将所述访问请求的相关信息生成第一指纹信息；

接收所述服务器系统发送的标识信息，所述标识信息中携带有所述第一指纹信息；

将所述标识信息携带在用于请求对访问行为进行记录的日志记录请求中向所述服务

器系统发送，以便所述服务器系统通过指纹算法将所述访问行为的相关信息生成第二指纹信息，在所述日志记录请求满足记录条件的情况下按照所述日志记录请求将所述访问行为记录到网站访问日志，在所述日志记录不满足所述记录条件的情况下拒绝按照所述日志记录请求将所述访问行为记录到网站访问日志；

其中，所述记录条件为：所述日志记录请求中携带有所述标识信息且所述第一指纹信息与所述第二指纹信息相同。

第四方面，本申请实施例提供了一种记录网站访问日志的装置，配置于服务器系统，包括：

第一接收单元，用于接收客户端发送的访问请求；

第一获取单元，用于获取所述访问请求的相关信息；

第一生成单元，用于通过指纹算法，将所述访问请求的相关信息生成第一指纹信息；

发送单元，用于向所述客户端发送携带有所述第一指纹信息的标识信息；

第二接收单元，用于接收日志记录请求，所述日志记录请求用于请求对访问行为进行记录；

第二获取单元，用于获取所述访问行为的相关信息；

第二生成单元，用于通过所述指纹算法，将所述访问行为的相关信息生成第二指纹信息；

记录单元，用于若所述日志记录请求满足记录条件，按照所述日志记录请求将所述访问行为记录到网站访问日志；

拒绝单元，用于若所述日志记录请求不满足记录条件，拒绝按照所述日志记录请求将所述访问行为记录到网站访问日志；

其中，所述记录条件为：所述日志记录请求中携带有所述标识信息且所述第一指纹信息与所述第二指纹信息相同。

第五方面，本申请实施例提供了一种记录网站访问日志的装置，配置于客户端，包括：

第一发送单元，用于向服务器系统发送访问请求，以便所述服务器系统获取所述访问请求的相关信息并通过指纹算法将所述访问请求的相关信息生成第一指纹信息；

接收单元，用于接收所述服务器系统发送的标识信息，所述标识信息中携带有所述第一指纹信息；

第二发送单元，用于将所述标识信息携带在用于请求对访问行为进行记录的日志记

录请求中向所述服务器系统发送，以便所述服务器系统通过指纹算法将所述访问行为的相关信息生成第二指纹信息，在所述日志记录请求满足记录条件的情况下按照所述日志记录请求将所述访问行为记录到网站访问日志，在所述日志记录不满足所述记录条件的情况下拒绝按照所述日志记录请求将所述访问行为记录到网站访问日志；

其中，所述记录条件为：所述日志记录请求中携带有所述标识信息且所述第一指纹信息与所述第二指纹信息相同。

与现有技术相比，本申请具有以下优点：

根据本申请实施例的技术方案，网站的服务器系统可以在记录访问行为的过程中增加访问请求的指纹校验。通过指纹校验的结果服务器系统可以确定请求记录的访问行为是否对应于服务器系统曾经接收到过的访问请求，从而能够准确地区分用户请求记录的访问行为是否真实发生过。具体地，网站的服务器系统在接收到客户端发送的访问请求的情况下，可以基于该访问请求的相关信息生成第一指纹信息并携带在标识信息中返回给客户端，以指示客户端在请求记录该访问请求对应的访问行为时将该标识信息携带在日志记录请求中向服务器系统发送。网站的服务器系统在接收到用于请求对访问行为进行记录的日志记录请求的情况下，可以基于日志记录请求对应的访问行为的相关信息生成第二指纹信息并分析该日志记录请求是否满足记录条件，从而确定是否按照该日志请求记录将该访问行为记录到网站访问日志。其中，第一指纹信息和第二指纹信息是采用相同的指纹算法生成的；所述记录条件为：该日志记录请求中携带有标识信息且第一指纹信息与第二指纹信息相同。可以理解的是，若日志记录请求没有携带标识信息或者第二指纹信息与日志记录请求携带的第一指纹信息不相同，则网站的服务器系统没有接收到过该日志记录请求所请求记录的访问行为对应的访问请求，可见，该访问行为是没有真实发生过的。若日志记录请求携带有标识信息且第二指纹信息与日志记录请求携带的第一指纹信息相同，则网站的服务器系统接收到过该日志记录请求所请求记录的访问行为对应的访问请求，可见，该访问行为是真实发生过的。由此可见，网站的服务器在接收到用户的日志记录请求时能够准确地区分用户请求记录的访问行为是否真实发生过，从而就可以避免没有真实发生过的用户访问行为被记录到网站访问日志。

附图说明

为了更清楚地说明本申请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

申请中记载的一些实施例，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。

图 1 为本申请实施例中一应用场景所涉及的网络系统框架示意图；

图 2 为本申请实施例中一种记录网站访问日志的系统的结构示意图；

图 3 为本申请实施例中一种记录网站访问日志的方法的流程示意图；

图 4 为本申请实施例中一种记录网站访问日志的方法的流程示意图；

图 5 为本申请实施例中一种记录网站访问日志的方法的流程示意图；

图 6 为本申请实施例中一种记录网站访问日志的装置的结构示意图；

图 7 为本申请实施例中一种记录网站访问日志的装置的结构示意图。

具体实施方式

为了使本技术领域的人员更好地理解本申请方案，下面将结合本申请实施例中的附图，对本申请实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅是本申请一部分实施例，而不是全部的实施例。基于本申请中的实施例，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，都属于本申请保护的范围。

本申请可用于众多通用或专用的计算系统环境或配置中。例如：个人计算机、服务器计算机、手持设备或便携式设备、平板型设备、多处理器系统、基于微处理器的系统、置顶盒、可编程的消费电子设备、网络 PC、小型计算机、大型计算机、包括以上任何系统或设备的分布式计算环境等等。

本申请可以在由计算机执行的计算机可执行指令的一般上下文中描述，例如程序模块。一般地，程序模块包括执行特定任务或实现特定抽象数据类型的例程、程序、对象、组件、数据结构等等。也可以在分布式计环境中实践本申请，在这些分布式计算环境中，由通过通信网络而被连接的远程处理设备来执行任务。在分布式计算环境中，程序模块可以位于包括存储设备在内的本地和远程计算机存储介质中。

本申请的发明人经过研究发现，有些用户会在实际上没有对网站信息进行访问的情况下伪造与访问请求对应的日志记录请求并向网站的服务器发送，以期网站的服务器将实际上没有真实发生过的用户访问行为记录到网站访问日志，从而达到刷网页访问流量等恶意行为。但是，网站的服务器在接收到用户的日志记录请求时往往无法准确地区分用户请求记录的用户访问行为是否真实发生过，因此，网站的服务器难以避免地会将没有真实发生过的用户访问行为记录到网站访问日志。

为了解决现有技术的上述问题，在本申请实施例中，网站的服务器系统可以在记录访问行为的过程中增加访问请求的指纹校验。通过指纹校验的结果服务器系统可以确定请求记录的访问行为是否对应于服务器系统曾经接收到过的访问请求，从而能够准确地区分用户请求记录的访问行为是否真实发生过。具体地，网站的服务器系统在接收到客户端发送的访问请求的情况下，可以基于访问请求的相关信息生成第一指纹信息并返回给客户端。网站的服务器系统在接收到日志记录请求的情况下，可以基于访问行为的相关信息生成第二指纹信息并判断第二指纹信息是否与该日志记录请求中携带的第一指纹信息相同，从而确定是否按照该日志请求记录将该访问行为记录到网站访问日志。可以理解的是，若日志记录请求没有携带标识信息或者第二指纹信息与日志记录请求携带的第一指纹信息不相同，则网站的服务器系统没有接收到过该访问行为对应的访问请求，可见，该访问行为是没有真实发生过的，而是用户在实际上没有对网站信息进行访问的情况下伪造出来的。若日志记录请求携带有标识信息且第二指纹信息与日志记录请求携带的第一指纹信息相同，则网站的服务器系统接收到过该日志记录请求所请求记录的访问行为对应的访问请求，可见，该访问行为是真实发生过的。由此可见，网站的服务器在接收到用户的日志记录请求时能够准确地区分用户请求记录的访问行为是否真实发生过，从而就可以避免没有真实发生过的用户访问行为被记录到网站访问日志。

举例说明，本申请实施例的场景之一，例如可以是应用到如图 1 所示的应用场景。在该应用场景中，用户可以通过客户端 102 对服务器系统 101 提供的网站进行访问，其中，网站的服务器系统 101 可以与客户端 102 进行交互。

在图 1 所示的应用场景中，客户端 102 可以向服务器系统 101 发送访问请求，其中，所述访问请求中携带有所述访问请求的相关信息。服务器系统 101 在获取到访问请求的相关信息之后，可以通过指纹算法将所述访问请求的相关信息生成第一指纹信息，并向客户端 102 发送携带有所述第一指纹信息的标识信息。客户端 102 在获取所述标识信息之后，可以向服务器系统 101 发送日志记录请求，其中，所述日志记录请求用于请求对所述访问请求对应的访问行为进行记录，所述日志记录请求中携带有所述访问行为的相关信息以及所述标识信息。服务器系统 101 在获取所述访问行为的相关信息之后，可以通过所述指纹算法将所述访问行为的相关信息生成第二指纹信息。若所述日志记录请求满足记录条件，服务器系统 101 可以按照所述日志记录请求将所述访问行为记录到网站访问日志。若所述日志记录请求不满足记录条件，服务器系统 101 可以拒绝按照所述日志记录请求将所述访问行为记录到网站访问日志。其中，所述记录条件为：所述日志记

录请求中携带有所述标识信息且所述第一指纹信息与所述第二指纹信息相同。

可以理解的是，上述场景仅是本申请实施例提供的一个场景示例，本申请实施例并不限于此场景。

下面结合附图，详细说明本申请的各种非限制性实施方式。

示例性系统

参见图 2，示出了本申请实施例中一种记录网站访问日志的系统的结构示意图。所述系统例如具体可以包括客户端 202 和服务器系统 201；

所述服务器系统 201，用于接收所述客户端 202 发送的访问请求并获取所述访问请求的相关信息，通过指纹算法将所述访问请求的相关信息生成第一指纹信息，向所述客户端 202 发送携带有所述第一指纹信息的标识信息，接收用于请求对访问行为进行记录的日志记录请求并获取所述访问行为的相关信息，通过所述指纹算法将所述访问行为的相关信息生成第二指纹信息，若所述日志记录满足记录条件则按照所述日志记录请求将所述访问行为记录到网站访问日志，若所述日志记录不满足记录条件则拒绝按照所述日志记录请求将所述访问行为记录到网站访问日志；

所述客户端 202，用于向所述服务器系统 201 发送访问请求并接收所述服务器系统 201 针对所述访问请求返回的所述标识信息，将所述标识信息携带在所述日志访问请求中向所述服务器系统 201 发送；

其中，所述记录条件为：所述日志记录请求中携带有所述标识信息且所述第一指纹信息与所述第二指纹信息相同。

可选的，

所述访问请求的相关信息包括所述访问请求对应的用户 IP 地址和/或所述访问请求对应的访问时间；

所述访问行为的相关信息包括所述访问行为对应的用户 IP 地址和/或所述访问行为对应的访问时间。

可选的，

所述访问请求的相关信息还包括所述访问请求对应的引用页 referer 标识和进入页 entry 标识；

所述访问行为的相关信息还包括所述访问行为对应的 referer 标识和 entry 标识。

可选的，

所述访问请求对应的 referer 标识具体为所述访问请求对应的 referer 地址的哈希值，所述访问请求对应的 entry 标识具体为所述访问请求对应的 entry 地址的哈希值；

所述访问行为对应的 referer 标识具体为所述访问行为对应的 referer 地址的哈希值，所述访问行为对应的 entry 标识具体为所述访问行为对应的 entry 地址的哈希值。

可选的，

所述标识信息还携带有所述访问请求对应的 referer 标识和 entry 标识；

所述记录条件具体为：所述日志记录请求中携带有所述标识信息，所述第一指纹信息与所述第二指纹信息相同，所述访问请求对应的 referer 标识与所述访问行为对应的 referer 标识相同，以及，所述访问请求对应的 entry 标识与所述访问行为对应的 entry 标识。

可选的，

所述标识信息还携带有所述访问请求对应的访问时间；

所述记录条件具体为：所述日志记录请求中携带有所述标识信息，所述第一指纹信息与所述第二指纹信息相同，以及，当前时间与所述访问请求对应的访问时间之间的时间差不超过有效时间阈值。

在本实施例中，网站的服务器在接收到用户的日志记录请求时能够准确地区分用户请求记录的访问行为是否真实发生过，从而就可以避免没有真实发生过的用户访问行为被记录到网站访问日志。

示例性方法

参见图 3，示出了本申请实施例中一种记录网站访问日志的方法的流程示意图。本实施例的方法可以应用于服务器系统，如网站的服务器系统。所述方法例如具体可以包括以下步骤：

301、接收客户端发送的访问请求并获取所述访问请求的相关信息。

302、通过指纹算法，将所述访问请求的相关信息生成第一指纹信息。

303、向所述客户端发送携带有所述第一指纹信息的标识信息。

在本实施例中，在客户端向服务器系统发送访问请求时，服务器系统可以从访问请求中提取一些相关信息并通过指纹算法将提取出的相关信息生成第一指纹信息。然后，服务器系统可以生成携带有第一指纹信息的标识信息并向客户端发送。其中，所述标识信息用于携带在该访问请求对应的日志记录请求中，以便服务器系统基于第一指纹信息

对该日志记录请求进行指纹校验。其中，该访问请求对应的日志记录请求用于对该访问请求对应的访问行为进行记录。

可以理解的是，在不同的场景下，在所述标识信息发送给客户端之后，客户端可能会对所述标识信息采用不同的处理方式，因此，服务器系统可能会接收到不同的日志记录请求。

例如，若客户端要请求对在所述访问请求下产生的真实访问行为进行记录，客户端可以将所述标识信息携带在用于请求对所述访问请求对应的真实访问行为的日志记录请求中向服务器系统发送。在所述日志记录请求中还携带有所述真实访问行为的相关信息。由于所述真实访问行为与所述访问请求是相对应的，即所述真实访问行为是在所述访问请求下产生的，因此，所述真实访问行为的相关信息与所述访问请求的相关信息相同。

又如，若客户端要请求对并非在所述访问请求下产生的伪造访问行为进行记录，客户端可能将所述标识信息携带在用于请求对所述访问请求不对应的伪造访问行为的日志记录请求中向服务器系统发送。在所述日志记录请求中还携带有所述伪造访问行为的相关信息。由于所述伪造访问行为与所述访问请求是不对应的，即所述伪造访问行为并不是在所述访问请求下产生的，因此，所述伪造访问行为的相关信息与所述访问请求的相关信息并不相同。

再如，若客户端要请求对并非在所述访问请求下产生的伪造访问行为进行记录，客户端可能在用于请求对所述访问请求不对应的伪造访问行为的日志记录请求中不携带所述标识信息的情况下向服务器系统发送所述日志记录请求。因此，在服务器系统中接收到的日志记录请求中没有携带所述标识信息。

304、接收日志记录请求并获取访问行为的相关信息，所述日志记录请求用于请求对所述访问行为进行记录。

305、通过所述指纹算法，将所述访问行为的相关信息生成第二指纹信息。

306、若所述日志记录请求满足记录条件，按照所述日志记录请求将所述访问行为记录到网站访问日志。

307、若所述日志记录请求不满足记录条件，拒绝按照所述日志记录请求将所述访问行为记录到网站访问日志。

其中，所述记录条件为：所述日志记录请求中携带有所述标识信息且所述第一指纹信息与所述第二指纹信息相同。

具体实现时，在接收到客户端发送的日志记录请求时，服务器系统可以判断所述日

志记录请求中是否携带有标识信息。若所述日志记录请求没有携带所述标识信息，则执行步骤 307。若所述日志记录请求携带有标识信息，服务器系统可以判断标识信息中是否携带有第一指纹信息。若标识信息中携带有第一指纹信息，则执行步骤 307。若标识信息中携带有第一指纹信息，服务器系统可以从日志记录请求中获取其请求记录的访问行为的一些相关信息并通过指纹算法将提取出的相关信息生成第二指纹信息，然后判断第一指纹信息与第二指纹信息是否相同，若相同则执行步骤 306，若不相同则执行步骤 307。

可以理解的是，若客户端发起的日志记录请求是用于请求对伪造访问行为进行记录，由于伪造访问行为并不是在服务器系统接收到过的访问请求下产生的真实访问行为，而为了达到刷网页访问流量的目的，伪造访问行为的相关信息需要与服务器系统接收到过的访问请求的相关信息存在区别，因此，基于相同的指纹算法，第一指纹信息与第二指纹信息是不相同的。可见，对于服务器系统接收到的日志记录请求来说，若判断出第一指纹信息与第二指纹信息不相同，则可以确定该日志记录请求所请求记录的访问行为是伪造的访问行为而并非真实发生过的访问行为，从而可以拒绝将该访问行为记录到网站访问日志。若客户端发起的日志记录请求是用于请求对在访问请求下产生的真实访问行为，则真实访问行为的相关信息与服务器接收到过的访问请求的相关信息是相同的，因此，基于相同的指纹算法，第一指纹信息与第二指纹信息是相同的。可见，对于服务器系统接收到的日志记录请求来说，若判断出第一指纹信息与第二指纹信息相同，则可以确定该日志记录请求所请求记录的访问行为是真实发生过的访问行为，从而可以将该访问行为记录到网站访问日志。

在本实施例中，所述访问请求的相关信息表示用于生成第一指纹信息的信息，所述访问行为的相关信息表示用于生成第二指纹信息的信息。由于访问请求的相关信息能够用于描述所述访问请求，访问行为的相关信息能够用于描述所述访问行为，因此，第一指纹信息能够起到标识所述访问请求的作用，第二指纹信息能够起到标识所述访问行为的作用。因此，第一指纹信息与第二指纹信息能够用于区分所述访问行为是否是在所述访问请求下产生的行为，从而实现针对日志记录请求的指纹校验。

在本实施例中，所述访问请求的多种不同的相关信息可以用于生成第一指纹信息，相应地，所述访问行为的多种不同的相关信息可以用于生成第二指纹信息。

例如，访问行为的伪造可以通过修改真实发生过的访问请求对应的用户 IP 地址来实现，伪造的访问行为与真实的访问请求往往具有不同的用户 IP 地址。因此，在本实施例

的一些实施方式中，所述访问请求对应的用户 IP 地址可以用于生成第一指纹信息，相应地，所述访问行为对应的用户 IP 地址可以用于生成第二指纹信息，也即，所述访问请求的相关信息可以包括访问请求对应的用户 IP 地址，相应地，所述访问行为的相关信息可以包括访问行为对应的用户 IP 地址。

又如，访问行为的伪造也可以通过修改真实发生过的访问请求对应的访问时间来实现，伪造的访问行为与真实的访问请求往往具有不同的访问时间。因此，在本实施例的另一些实施方式中，所述访问请求对应的访问时间可以用于生成第一指纹信息，相应地，所述访问行为对应的访问时间可以用于生成第二指纹信息，也即，所述访问请求的相关信息可以包括访问请求对应的访问时间，相应地，所述访问行为的相关信息可以包括访问行为对应的访问时间。

再如，在用户通过搜索关键词来访问网站时，访问行为的伪造也可以通过修改真实发生过的访问请求对应的搜索关键词来实现，伪造的访问行为与真实的访问请求往往具有不同的搜索关键词。因此，在本实施例的又一些实施方式中，所述访问请求对应的搜索关键词可以用于生成第一指纹信息，相应地，所述访问行为对应的搜索关键词可以用于生成第二指纹信息，也即，所述访问请求的相关信息可以包括访问请求对应的搜索关键词，相应地，所述访问行为的相关信息可以包括访问行为对应的搜索关键词。

又再如，访问行为的伪造也可以通过修改真实发生过的访问请求对应的引用页 referer 和进入页 entry 来实现，伪造的访问行为与真实的访问请求往往具有不同的 referer 标识和不同的 entry 标识。因此，在本实施例的又一些实施方式中，所述访问请求对应的 referer 标识和 entry 标识可以用于生成第一指纹信息，相应地，所述访问行为对应的 referer 标识和 entry 标识可以用于生成第二指纹信息，也即，所述访问请求的相关信息可以包括访问请求对应的 referer 标识和 entry 标识，相应地，所述访问行为的相关信息可以包括访问行为对应的 referer 标识和 entry 标识。其中，referer 也可以称为来源页，entry 也可以称谓当前页。对于一个访问请求来说，用户是在访问 referer 时请求访问 entry；对于一个访问行为来说，用户当前访问的网页是 entry，用户在当前网页之前访问的网页是 referer。此外，为了便于 referer 标识与 entry 标识用于生成指纹信息，referer 标识可以是 referer 地址 url 的哈希值，entry 标识可以是 entry 地址 url 的哈希值。具体地，所述访问请求对应的 referer 标识具体可以是所述访问请求对应的 referer 地址的哈希值，所述访问请求对应的 entry 标识具体可以是所述访问请求对应的 entry 地址的哈希值，相应地，所述访问行为对应的 referer 标识具体可以是所述访问行为对应的 referer 地址的哈希值，所

述访问行为对应的 entry 标识具体可以是所述访问行为对应的 entry 地址的哈希值。

可以理解的是，所述第一指纹信息和所述第二指纹信息可以由上述提及的任意一种或多种信息生成，也即，所述访问请求的相关信息和所述访问行为的相关信息可以包括上述提及的任意一种或多种信息。例如，所述第一指纹信息可以由所述访问请求对应的用户 IP 地址、访问时间、referer 标识和 entry 标识生成，即所述访问请求的相关信息可以包括所述访问请求对应的用户 IP 地址、访问时间、referer 标识和 entry 标识，相应地，所述第二指纹信息可以由所述访问行为对应的用户 IP 地址、访问时间、referer 标识和 entry 标识生成，即所述访问行为的相关信息可以包括所述访问行为对应的用户 IP 地址、访问时间、referer 标识和 entry 标识。进一步而言，在所述第一指纹信息包括所述访问请求的多种相关信息的情况下，所述访问请求的多种相关信息例如可以通过锚点符号等方式连接成一个字符串，该字符串即是所述第一指纹信息。例如，所述访问请求对应的用户 IP 地址、访问时间、referer 地址的哈希值和 entry 地址的哈希值可以通过锚点符号等方式连接成所述第一指纹信息。相应地，在所述第二指纹信息包括所述访问行为的多种相关信息的情况下，所述访问行为的多种相关信息例如可以通过锚点符号等方式连接成一个字符串，该字符串即是所述第二指纹信息。例如，所述访问行为对应的用户 IP 地址、访问时间、referer 地址的哈希值和 entry 地址的哈希值可以通过锚点符号等方式连接成所述第二指纹信息。

在本实施例的一些实施方式中，在指纹校验的基础上，还可以进一步通过其他的校验方式对日志记录请求进行校验，以进一步识别日志记录请求所请求记录的访问行为是否真实发生过。

例如，服务器系统除了验证日志记录请求中是否携带有所述标识信息以及所述第一指纹信息与所述第二指纹信息是否相同之外，还可以验证所述访问行为对应的 referer、entry 是否与所述访问请求对应的 referer、entry 相同。具体地，所述标识信息除了携带有所述第一指纹信息之外，还可以携带有 referer 标识和 entry 标识。所述记录条件具体可以包括：所述日志记录请求中携带有所述标识信息，所述第一指纹信息与所述第二指纹信息相同，所述访问请求对应的 referer 标识与所述访问行为对应的 referer 标识相同，以及，所述访问请求对应的 entry 标识与所述访问行为对应的 entry 标识。在这种情况下，在上述记录条件完全被满足的情况下执行 306，在上述记录条件没有被完全满足的情况下执行 307。例如，若所述第一指纹信息与所述第二指纹信息不相同，即使所述访问请求对应的 referer 标识、entry 标识与所述访问行为对应的 referer 标识、entry 标识均相同，

也会执行 307。又如，若所述访问请求对应的 referer 标识、entry 标识与所述访问行为对应的 referer 标识、entry 标识不相同，即使所述第一指纹信息与所述第二指纹信息相同，也会执行 307。

又如，服务器系统除了验证日志记录请求中是否携带有所述标识信息以及所述第一指纹信息与所述第二指纹信息是否相同之外，还可以要求客户端在访问请求发生之后一定的有效时间内发起日志记录请求，也即，服务器系统还可以验证所述访问请求对应的访问时间距离当前时间是否在有效时间阈值内。具体地，所述标识信息除了携带有所述第一指纹信息之外，还可以携带有所述访问请求对应的访问时间。所述记录条件具体可以包括：所述日志记录请求中携带有所述标识信息，所述第一指纹信息与所述第二指纹信息相同，以及，当前时间与所述访问请求对应的访问时间之间的时间差不超过有效时间阈值。在这种情况下，在上述记录条件完全被满足的情况下执行 306，在上述记录条件没有被完全满足的情况下执行 307。例如，若所述第一指纹信息与所述第二指纹信息不相同，即使当前时间与所述访问请求对应的访问时间之间的时间差不超过有效时间阈值，也会执行 307。又如，若当前时间与所述访问请求对应的访问时间之间的时间差超过了有效时间阈值，即使所述第一指纹信息与所述第二指纹信息相同，也会执行 307。

在本实施例中，所述客户端可以是运行在用户终端上的浏览器，或者也可以是运行在用户终端上的网络应用的客户端程序。在客户端为浏览器的情况下，所述标识信息具体可以是通过 JS 代码的形式由服务器系统发送给客户端并指示客户端发送日志记录请求。具体地，在服务器系统中，所述标识信息中要携带的各种信息可以通过锚点符号等方式生成一个字符串，并用 BASE64 对标识信息进行编码，编码后生成的特征串可以记为 SIGNATURE，该 SIGNATURE 即可以作为所述标识信息。SIGNATURE 可以作为参数 sig 插入到 BEACON 模块的 JS 代码中。服务器系统可以将该 JS 代码发送给客户端。客户端在执行 JS 代码的过程中可以收集访问行为的相关信息并基于访问行为的相关信息向服务器系统发送携带有参数 sig 的日志记录请求。服务器系统可以在接收到日志记录请求之后，通过解析参数 sig 可以获得 SIGNATURE，再用 BASE64 对 SIGNATURE 进行解码并使用锚点符号进行分解，可以得到所述标识信息中携带的各种信息。

可以理解的是，本实施例提及的服务器系统具体可以包括用于处理用户访问的网络应用服务器（Web Server）和用于处理访问行为记录的日志服务器（Log Server）。其中，网络应用服务器用于处理客户端的访问请求，即网络应用服务器用于执行 301、302 和 303。日志服务器用于处理客户端的日志记录请求，即日志服务器用于执行 304、305、

306 和 307。

在本实施例中，网站的服务器系统可以在记录访问行为的过程中增加访问请求的指纹校验。通过指纹校验的结果服务器系统可以确定请求记录的访问行为是否对应于服务器系统曾经接收到过的访问请求，从而能够准确地区分用户请求记录的访问行为是否真实发生过。具体地，网站的服务器系统在接收到客户端发送的访问请求的情况下，可以基于访问请求的相关信息生成第一指纹信息并返回给客户端。网站的服务器系统在接收到日志记录请求的情况下，可以基于访问行为的相关信息生成第二指纹信息并判断第二指纹信息是否与该日志记录请求中携带的第一指纹信息相同，从而确定是否按照该日志请求记录将该访问行为记录到网站访问日志。可以理解的是，若日志记录请求没有携带标识信息或者第二指纹信息与日志记录请求携带的第一指纹信息不相同，则网站的服务器系统没有接收到过该访问行为对应的访问请求，可见，该访问行为是没有真实发生过的，而是用户在实际上没有对网站信息进行访问的情况下伪造出来的。若日志记录请求携带有标识信息且第二指纹信息与日志记录请求携带的第一指纹信息相同，则网站的服务器系统接收到过该日志记录请求所请求记录的访问行为对应的访问请求，可见，该访问行为是真实发生过的。由此可见，网站的服务器在接收到用户的日志记录请求时能够准确地区分用户请求记录的访问行为是否真实发生过，从而就可以避免没有真实发生过的用户访问行为被记录到网站访问日志。

参见图 4，示出了本申请实施例中一种记录网站访问日志的方法的流程示意图。本实施例的方法可以应用于客户端。所述方法例如具体可以包括以下步骤：

401、向服务器系统发送访问请求，以便所述服务器系统获取所述访问请求的相关信息并通过指纹算法将所述访问请求的相关信息生成第一指纹信息；

402、接收所述服务器系统发送的标识信息，所述标识信息中携带有所述第一指纹信息；

403、将所述标识信息携带在用于请求对访问行为进行记录的日志记录请求中向所述服务器系统发送，以便所述服务器系统通过指纹算法将所述访问行为的相关信息生成第二指纹信息，在所述日志记录请求满足记录条件的情况下按照所述日志记录请求将所述访问行为记录到网站访问日志，在所述日志记录不满足所述记录条件的情况下拒绝按照所述日志记录请求将所述访问行为记录到网站访问日志；

其中，所述记录条件为：所述日志记录请求中携带有所述标识信息且所述第一指纹

信息与所述第二指纹信息相同。

可选的，

所述访问请求的相关信息包括所述访问请求对应的用户 IP 地址和/或所述访问请求对应的访问时间；

所述访问行为的相关信息包括所述访问行为对应的用户 IP 地址和/或所述访问行为对应的访问时间。

可选的，

所述访问请求的相关信息还包括所述访问请求对应的引用页 referer 标识和进入页 entry 标识；

所述访问行为的相关信息还包括所述访问行为对应的 referer 标识和 entry 标识。

可选的，

所述访问请求对应的 referer 标识具体为所述访问请求对应的 referer 地址的哈希值，所述访问请求对应的 entry 标识具体为所述访问请求对应的 entry 地址的哈希值；

所述访问行为对应的 referer 标识具体为所述访问行为对应的 referer 地址的哈希值，所述访问行为对应的 entry 标识具体为所述访问行为对应的 entry 地址的哈希值。

可选的，

所述标识信息还携带有所述访问请求对应的 referer 标识和 entry 标识；

所述记录条件具体为：所述日志记录请求中携带有所述标识信息，所述第一指纹信息与所述第二指纹信息相同，所述访问请求对应的 referer 标识与所述访问行为对应的 referer 标识相同，以及，所述访问请求对应的 entry 标识与所述访问行为对应的 entry 标识。

可选的，

所述标识信息还携带有所述访问请求对应的访问时间；

所述记录条件具体为：所述日志记录请求中携带有所述标识信息，所述第一指纹信息与所述第二指纹信息相同，以及，当前时间与所述访问请求对应的访问时间之间的时间差不超过有效时间阈值。

在本实施例中，网站的服务器在接收到用户的日志记录请求时能够准确地区分用户请求记录的访问行为是否真实发生过，从而就可以避免没有真实发生过的用户访问行为被记录到网站访问日志。

为了使得本领域技术人员更容易理解本申请实施例在实际场景中的实现方式，下面以一个场景为例进行介绍。在该场景中，网站的服务器系统包括网络应用服务器和日志服务器，网络应用服务器用于处理用户对网站的访问，日志服务器用于处理用户访问行为的记录。与服务器系统进行交互的客户端为用户终端上的浏览器。参见图 5，示出了本申请实施例中一种记录网站访问日志的方法的流程示意图。所述方法例如具体可以包括以下步骤：

501、用户浏览器向网络应用服务器发送访问请求。

502、网络应用服务器获取所述访问请求对应的 referer url 和 entry url，并通过 hash 算法分别对 referer url 和 entry url 进行计算，生成所述访问请求对应的 referer url 哈希值和 entry url 哈希值。

503、获取所述访问请求对应的用户 IP 地址和访问时间，将所述访问请求对应的用户 IP 地址、访问时间、referer url 哈希值和 entry url 哈希值连接成一个字符串。

其中，连接的方式例如可以是锚点符号。

504、网络应用服务器通过指纹算法，将 503 中生成的字符串生成第一指纹信息。

505、网络应用服务器将 503 中生成的字符串与第一指纹信息里连接成一个字符串，并用 BASE64 编码生成特征串 SIGNATURE。

其中，连接的方式例如可以是锚点符号。特征串 SIGNATURE 即是前述实施例提及的所述标识信息。

506、网络应用服务器将 SIGNATURE 作为参数 sig 插入到 BEACON 模块的 JS 代码中发送给用户浏览器。

507、用户浏览器通过解析和执行 JS 代码，收集访问行为的相关信息并向日志服务器发送携带有 SIGNATURE 的日志记录请求。

其中，所述日志记录请求中还携带有所述访问行为的相关信息。所述访问行为的相关信息可以包括所述访问行为对应的用户 IP 地址、访问时间、referer url 和 entry url。

508、日志服务器验证所述日志记录请求中携带的 SIGNATURE。

其中，若日志记录请求中携带的 SIGNATURE 为空值或非法的 BASE64 字符串，则进入 516。若日志记录请求中不存在 SIGNATURE，则进入 516。若日志记录请求中携带有 SIGNATURE 且 SIGNATURE 是合法的 BASE64 字符串，则进入 509。

509、日志服务器对所述日志记录请求中携带的 SIGNATURE 进行 BASE64 解码，生成一个字符串，并将该字符串分解成所述第一指纹信息以及所述访问请求对应的用户

IP 地址、访问时间、referer url 哈希值和 entry url 哈希值。

其中，分解的方式例如可以是锚点符号。

510、日志服务器验证当前时间与所述访问请求对应的访问时间之间的时间差是否超过有效时间阈值。

若该时间差超过有效时间阈值，则进入 516。若该时间差未超过有效时间阈值，则进入 511。

511、日志服务器获取所述访问行为对应的 referer url 和 entry url，并通过 hash 算法分别对 referer url 和 entry url 进行计算，生成所述访问行为对应的 referer url 哈希值和 entry url 哈希值。

512、日志服务器验证所述访问请求对应的 referer url 哈希值与所述访问行为对应的 referer url 哈希值是否相同以及所述访问请求对应的 entry url 哈希值与所述访问行为对应的 entry url 哈希值是否相同。

若所述访问请求对应的 referer url 哈希值与所述访问行为对应的 referer url 哈希值相同且所述访问请求对应的 entry url 哈希值与所述访问行为对应的 entry url 哈希值相同，则进入 513。若所述访问请求对应的 referer url 哈希值与所述访问行为对应的 referer url 哈希值不相同和/或所述访问请求对应的 entry url 哈希值与所述访问行为对应的 entry url 哈希值不相同，则进入 516。

513、日志服务器将所述访问行为对应的用户 IP 地址、访问时间、referer url 哈希值和 entry url 哈希值连接成一个字符串，并通过指纹算法将该字符串生成第二指纹信息。

514、日志服务器验证第一指纹信息与第二指纹信息是否相同。

若第一指纹信息与第二指纹信息相同，进入 515。若第一指纹信息与第二指纹信息不相同，进入 516。

515、日志服务器按照所述日志记录请求将所述访问行为记录到网站访问日志。

516、日志服务器拒绝按照所述日志记录请求将所述访问行为记录到网站访问日志。

在本实施例中，网站的服务器在接收到用户的日志记录请求时能够准确地区分用户请求记录的访问行为是否真实发生过，从而就可以避免没有真实发生过的用户访问行为被记录到网站访问日志。

示例性设备

参见图 6，示出了本申请实施例中一种记录网站访问日志的装置的结构示意图。本

实施例的装置可以配置于服务器系统，所述装置例如可以包括：

第一接收单元 601，用于接收客户端发送的访问请求；

第一获取单元 602，用于获取所述访问请求的相关信息；

第一生成单元 603，用于通过指纹算法，将所述访问请求的相关信息生成第一指纹信息；

发送单元 604，用于向所述客户端发送携带有所述第一指纹信息的标识信息；

第二接收单元 605，用于接收日志记录请求，所述日志记录请求用于请求对访问行为进行记录；

第二获取单元 606，用于获取所述访问行为的相关信息；

第二生成单元 607，用于通过所述指纹算法，将所述访问行为的相关信息生成第二指纹信息；

记录单元 608，用于若所述日志记录请求满足记录条件，按照所述日志记录请求将所述访问行为记录到网站访问日志；

拒绝单元 609，用于若所述日志记录请求不满足记录条件，拒绝按照所述日志记录请求将所述访问行为记录到网站访问日志；

其中，所述记录条件为：所述日志记录请求中携带有所述标识信息且所述第一指纹信息与所述第二指纹信息相同。

可选的，

所述访问请求的相关信息包括所述访问请求对应的用户 IP 地址和/或所述访问请求对应的访问时间；

所述访问行为的相关信息包括所述访问行为对应的用户 IP 地址和/或所述访问行为对应的访问时间。

可选的，

所述访问请求的相关信息还包括所述访问请求对应的引用页 referer 标识和进入页 entry 标识；

所述访问行为的相关信息还包括所述访问行为对应的 referer 标识和 entry 标识。

可选的，

所述访问请求对应的 referer 标识具体为所述访问请求对应的 referer 地址的哈希值，所述访问请求对应的 entry 标识具体为所述访问请求对应的 entry 地址的哈希值；

所述访问行为对应的 referer 标识具体为所述访问行为对应的 referer 地址的哈希值，

所述访问行为对应的 entry 标识具体为所述访问行为对应的 entry 地址的哈希值。

可选的，

所述标识信息还携带有所述访问请求对应的 referer 标识和 entry 标识；

所述记录条件具体为：所述日志记录请求中携带有所述标识信息，所述第一指纹信息与所述第二指纹信息相同，所述访问请求对应的 referer 标识与所述访问行为对应的 referer 标识相同，以及，所述访问请求对应的 entry 标识与所述访问行为对应的 entry 标识。

可选的，

所述标识信息还携带有所述访问请求对应的访问时间；

所述记录条件具体为：所述日志记录请求中携带有所述标识信息，所述第一指纹信息与所述第二指纹信息相同，以及，当前时间与所述访问请求对应的访问时间之间的时间差不超过有效时间阈值。

在本实施例中，网站的服务器在接收到用户的日志记录请求时能够准确地区分用户请求记录的访问行为是否真实发生过，从而就可以避免没有真实发生过的用户访问行为被记录到网站访问日志。

参见图 7，示出了本申请实施例中一种记录网站访问日志的装置的结构示意图。本实施例的装置可以配置于客户端，所述装置例如可以包括：

第一发送单元 701，用于向服务器系统发送访问请求，以便所述服务器系统获取所述访问请求的相关信息并通过指纹算法将所述访问请求的相关信息生成第一指纹信息；

接收单元 702，用于接收所述服务器系统发送的标识信息，所述标识信息中携带有所述第一指纹信息；

第二发送单元 703，用于将所述标识信息携带在用于请求对访问行为进行记录的日志记录请求中向所述服务器系统发送，以便所述服务器系统通过指纹算法将所述访问行为的相关信息生成第二指纹信息，在所述日志记录请求满足记录条件的情况下按照所述日志记录请求将所述访问行为记录到网站访问日志，在所述日志记录不满足所述记录条件的情况下拒绝按照所述日志记录请求将所述访问行为记录到网站访问日志；

其中，所述记录条件为：所述日志记录请求中携带有所述标识信息且所述第一指纹信息与所述第二指纹信息相同。

可选的，

所述访问请求的相关信息包括所述访问请求对应的用户 IP 地址和/或所述访问请求对应的访问时间；

所述访问行为的相关信息包括所述访问行为对应的用户 IP 地址和/或所述访问行为对应的访问时间。

可选的，

所述访问请求的相关信息还包括所述访问请求对应的引用页 referer 标识和进入页 entry 标识；

所述访问行为的相关信息还包括所述访问行为对应的 referer 标识和 entry 标识。

可选的，

所述访问请求对应的 referer 标识具体为所述访问请求对应的 referer 地址的哈希值，所述访问请求对应的 entry 标识具体为所述访问请求对应的 entry 地址的哈希值；

所述访问行为对应的 referer 标识具体为所述访问行为对应的 referer 地址的哈希值，所述访问行为对应的 entry 标识具体为所述访问行为对应的 entry 地址的哈希值。

可选的，

所述标识信息还携带有所述访问请求对应的 referer 标识和 entry 标识；

所述记录条件具体为：所述日志记录请求中携带有所述标识信息，所述第一指纹信息与所述第二指纹信息相同，所述访问请求对应的 referer 标识与所述访问行为对应的 referer 标识相同，以及，所述访问请求对应的 entry 标识与所述访问行为对应的 entry 标识。

可选的，

所述标识信息还携带有所述访问请求对应的访问时间；

所述记录条件具体为：所述日志记录请求中携带有所述标识信息，所述第一指纹信息与所述第二指纹信息相同，以及，当前时间与所述访问请求对应的访问时间之间的时间差不超过有效时间阈值。

在本实施例中，网站的服务器在接收到用户的日志记录请求时能够准确地区分用户请求记录的访问行为是否真实发生过，从而就可以避免没有真实发生过的用户访问行为被记录到网站访问日志。

需要说明的是，在本文中，诸如第一和第二等之类的关系术语仅仅用来将一个实体或者操作与另一个实体或操作区分开来，而不一定要求或者暗示这些实体或操作之间存

在任何这种实际的关系或者顺序。术语“包括”、“包含”或者其任何其他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、物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他要素，或者是还包括为这种过程、方法、物品或者设备所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括所述要素的过程、方法、物品或者设备中还存在另外的相同要素。

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。以上所描述的设备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。

以上所述仅是本申请的具体实施方式，应当指出，对于本技术领域的普通技术人员来说，在不脱离本申请原理的前提下，还可以做出若干改进和润饰，这些改进和润饰也应视为本申请的保护范围。

权 利 要 求 书

1.一种记录网站访问日志的系统，其特征在于，包括客户端和服务器系统；

所述服务器系统，用于接收所述客户端发送的访问请求并获取所述访问请求的相关信息，通过指纹算法将所述访问请求的相关信息生成第一指纹信息，向所述客户端发送携带有所述第一指纹信息的标识信息，接收用于请求对访问行为进行记录的日志记录请求并获取所述访问行为的相关信息，通过所述指纹算法将所述访问行为的相关信息生成第二指纹信息，若所述日志记录满足记录条件则按照所述日志记录请求将所述访问行为记录到网站访问日志，若所述日志记录不满足记录条件则拒绝按照所述日志记录请求将所述访问行为记录到网站访问日志；

所述客户端，用于向所述服务器系统发送访问请求并接收所述服务器系统针对所述访问请求返回的所述标识信息，将所述标识信息携带在所述日志访问请求中向所述服务器系统发送；

其中，所述记录条件为：所述日志记录请求中携带有所述标识信息且所述第一指纹信息与所述第二指纹信息相同。

2.根据权利要求 1 所述的记录网站访问日志的系统，其特征在于，

所述访问请求的相关信息包括所述访问请求对应的用户 IP 地址和/或所述访问请求对应的访问时间；

所述访问行为的相关信息包括所述访问行为对应的用户 IP 地址和/或所述访问行为对应的访问时间。

3.根据权利要求 2 所述的记录网站访问日志的系统，其特征在于，

所述访问请求的相关信息还包括所述访问请求对应的引用页 referer 标识和进入页 entry 标识；

所述访问行为的相关信息还包括所述访问行为对应的 referer 标识和 entry 标识。

4.根据权利要求 3 所述的记录网站访问日志的系统，其特征在于，

所述访问请求对应的 referer 标识具体为所述访问请求对应的 referer 地址的哈希值，所述访问请求对应的 entry 标识具体为所述访问请求对应的 entry 地址的哈希值；

所述访问行为对应的 referer 标识具体为所述访问行为对应的 referer 地址的哈希值，所述访问行为对应的 entry 标识具体为所述访问行为对应的 entry 地址的哈希值。

5.根据权利要求 1、3 或 4 所述的记录网站访问日志的系统，其特征在于，

所述标识信息还携带有所述访问请求对应的 referer 标识和 entry 标识；

所述记录条件具体为：所述日志记录请求中携带有所述标识信息，所述第一指纹信息与所述第二指纹信息相同，所述访问请求对应的 referer 标识与所述访问行为对应的 referer 标识相同，以及，所述访问请求对应的 entry 标识与所述访问行为对应的 entry 标识。

6.根据权利要求 1 或 2 所述的记录网站访问日志的系统，其特征在于，

所述标识信息还携带有所述访问请求对应的访问时间；

所述记录条件具体为：所述日志记录请求中携带有所述标识信息，所述第一指纹信息与所述第二指纹信息相同，以及，当前时间与所述访问请求对应的访问时间之间的时间差不超过有效时间阈值。

7.一种记录网站访问日志的方法，其特征在于，应用于服务器系统，包括：

接收客户端发送的访问请求并获取所述访问请求的相关信息；

通过指纹算法，将所述访问请求的相关信息生成第一指纹信息；

向所述客户端发送携带有所述第一指纹信息的标识信息；

接收日志记录请求并获取访问行为的相关信息，所述日志记录请求用于请求对所述访问行为进行记录；

通过所述指纹算法，将所述访问行为的相关信息生成第二指纹信息；

若所述日志记录请求满足记录条件，按照所述日志记录请求将所述访问行为记录到网站访问日志；

若所述日志记录请求不满足记录条件，拒绝按照所述日志记录请求将所述访问行为记录到网站访问日志；

其中，所述记录条件为：所述日志记录请求中携带有所述标识信息且所述第一指纹信息与所述第二指纹信息相同。

8.根据权利要求 7 所述的方法，其特征在于，

所述访问请求的相关信息包括所述访问请求对应的用户 IP 地址和/或所述访问请求对应的访问时间；

所述访问行为的相关信息包括所述访问行为对应的用户 IP 地址和/或所述访问行为对应的访问时间。

9.根据权利要求 8 所述的方法，其特征在于，

所述访问请求的相关信息还包括所述访问请求对应的引用页 referer 标识和进入页 entry 标识；

所述访问行为的相关信息还包括所述访问行为对应的 referer 标识和 entry 标识。

10.根据权利要求 9 所述的方法，其特征在于，

所述访问请求对应的 referer 标识具体为所述访问请求对应的 referer 地址的哈希值，所述访问请求对应的 entry 标识具体为所述访问请求对应的 entry 地址的哈希值；

所述访问行为对应的 referer 标识具体为所述访问行为对应的 referer 地址的哈希值，所述访问行为对应的 entry 标识具体为所述访问行为对应的 entry 地址的哈希值。

11.根据权利要求 7、9 或 10 所述的方法，其特征在于，

所述标识信息还携带有所述访问请求对应的 referer 标识和 entry 标识；

所述记录条件具体为：所述日志记录请求中携带有所述标识信息，所述第一指纹信息与所述第二指纹信息相同，所述访问请求对应的 referer 标识与所述访问行为对应的 referer 标识相同，以及，所述访问请求对应的 entry 标识与所述访问行为对应的 entry 标识。

12.根据权利要求 7 或 8 所述的方法，其特征在于，

所述标识信息还携带有所述访问请求对应的访问时间；

所述记录条件具体为：所述日志记录请求中携带有所述标识信息，所述第一指纹信息与所述第二指纹信息相同，以及，当前时间与所述访问请求对应的访问时间之间的时间差不超过有效时间阈值。

13.一种记录网站访问日志的方法，其特征在于，应用于客户端，包括：

向服务器系统发送访问请求，以便所述服务器系统获取所述访问请求的相关信息并通过指纹算法将所述访问请求的相关信息生成第一指纹信息；

接收所述服务器系统发送的标识信息，所述标识信息中携带有所述第一指纹信息；

将所述标识信息携带在用于请求对访问行为进行记录的日志记录请求中向所述服务器系统发送，以便所述服务器系统通过指纹算法将所述访问行为的相关信息生成第二指纹信息，在所述日志记录请求满足记录条件的情况下按照所述日志记录请求将所述访问行为记录到网站访问日志，在所述日志记录不满足所述记录条件的情况下拒绝按照所述日志记录请求将所述访问行为记录到网站访问日志；

其中，所述记录条件为：所述日志记录请求中携带有所述标识信息且所述第一指纹信息与所述第二指纹信息相同。

14.根据权利要求 13 所述的方法，其特征在于，

所述访问请求的相关信息包括所述访问请求对应的用户 IP 地址和/或所述访问请求

对应的访问时间；

所述访问行为的相关信息包括所述访问行为对应的用户 IP 地址和/或所述访问行为对应的访问时间。

15.根据权利要求 14 所述的方法，其特征在于，

所述访问请求的相关信息还包括所述访问请求对应的引用页 referer 标识和进入页 entry 标识；

所述访问行为的相关信息还包括所述访问行为对应的 referer 标识和 entry 标识。

16.根据权利要求 15 所述的方法，其特征在于，

所述访问请求对应的 referer 标识具体为所述访问请求对应的 referer 地址的哈希值，所述访问请求对应的 entry 标识具体为所述访问请求对应的 entry 地址的哈希值；

所述访问行为对应的 referer 标识具体为所述访问行为对应的 referer 地址的哈希值，所述访问行为对应的 entry 标识具体为所述访问行为对应的 entry 地址的哈希值。

17.根据权利要求 13、15 或 16 所述的方法，其特征在于，

所述标识信息还携带有所述访问请求对应的 referer 标识和 entry 标识；

所述记录条件具体为：所述日志记录请求中携带有所述标识信息，所述第一指纹信息与所述第二指纹信息相同，所述访问请求对应的 referer 标识与所述访问行为对应的 referer 标识相同，以及，所述访问请求对应的 entry 标识与所述访问行为对应的 entry 标识。

18.根据权利要求 13 或 14 所述的方法，其特征在于，

所述标识信息还携带有所述访问请求对应的访问时间；

所述记录条件具体为：所述日志记录请求中携带有所述标识信息，所述第一指纹信息与所述第二指纹信息相同，以及，当前时间与所述访问请求对应的访问时间之间的时间差不超过有效时间阈值。

19.一种记录网站访问日志的装置，其特征在于，配置于服务器系统，包括：

第一接收单元，用于接收客户端发送的访问请求；

第一获取单元，用于获取所述访问请求的相关信息；

第一生成单元，用于通过指纹算法，将所述访问请求的相关信息生成第一指纹信息；

发送单元，用于向所述客户端发送携带有所述第一指纹信息的标识信息；

第二接收单元，用于接收日志记录请求，所述日志记录请求用于请求对访问行为进行记录；

第二获取单元，用于获取所述访问行为的相关信息；

第二生成单元，用于通过所述指纹算法，将所述访问行为的相关信息生成第二指纹信息；

记录单元，用于若所述日志记录请求满足记录条件，按照所述日志记录请求将所述访问行为记录到网站访问日志；

拒绝单元，用于若所述日志记录请求不满足记录条件，拒绝按照所述日志记录请求将所述访问行为记录到网站访问日志；

其中，所述记录条件为：所述日志记录请求中携带有所述标识信息且所述第一指纹信息与所述第二指纹信息相同。

20.一种记录网站访问日志的装置，其特征在于，配置于客户端，包括：

第一发送单元，用于向服务器系统发送访问请求，以便所述服务器系统获取所述访问请求的相关信息并通过指纹算法将所述访问请求的相关信息生成第一指纹信息；

接收单元，用于接收所述服务器系统发送的标识信息，所述标识信息中携带有所述第一指纹信息；

第二发送单元，用于将所述标识信息携带在用于请求对访问行为进行记录的日志记录请求中向所述服务器系统发送，以便所述服务器系统通过指纹算法将所述访问行为的相关信息生成第二指纹信息，在所述日志记录请求满足记录条件的情况下按照所述日志记录请求将所述访问行为记录到网站访问日志，在所述日志记录不满足所述记录条件的情况下拒绝按照所述日志记录请求将所述访问行为记录到网站访问日志；

其中，所述记录条件为：所述日志记录请求中携带有所述标识信息且所述第一指纹信息与所述第二指纹信息相同。

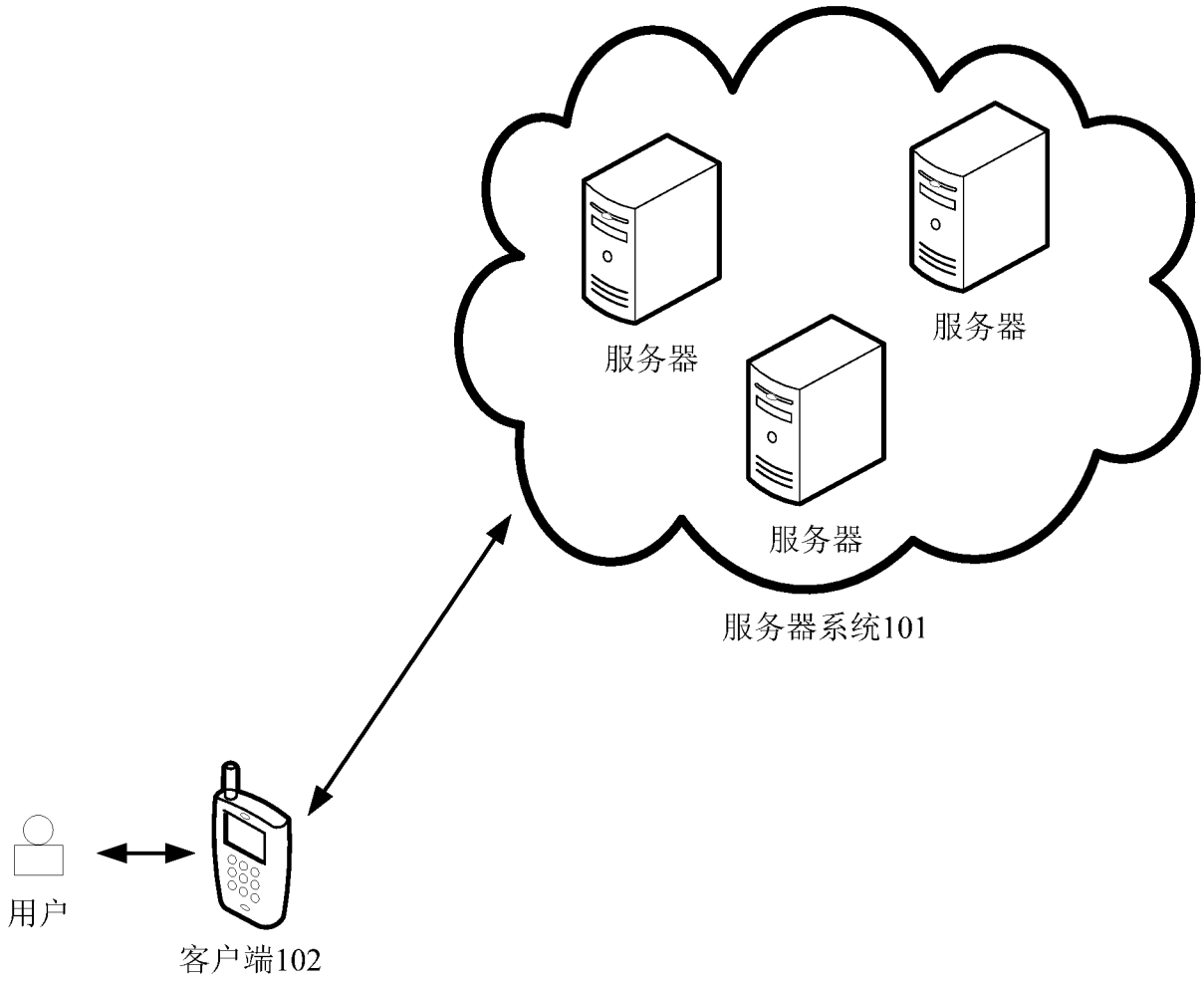


图 1

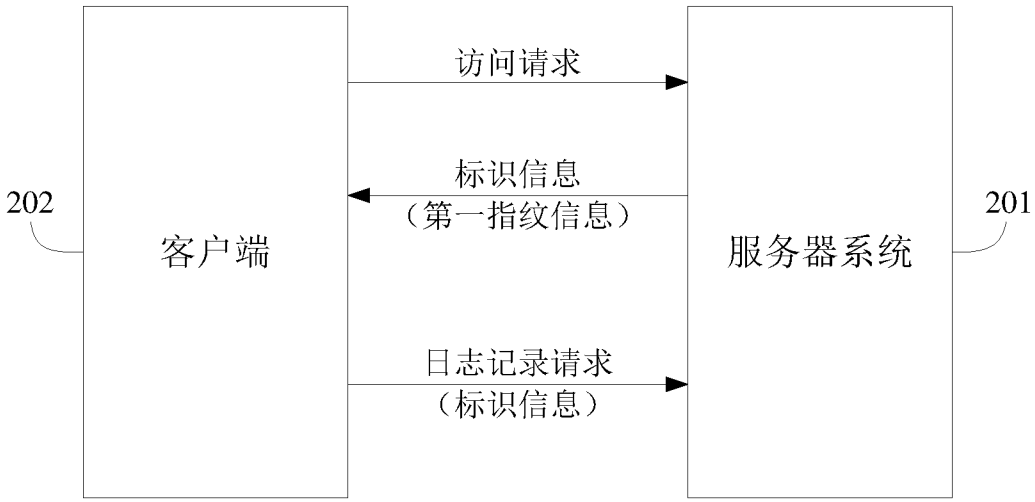


图 2

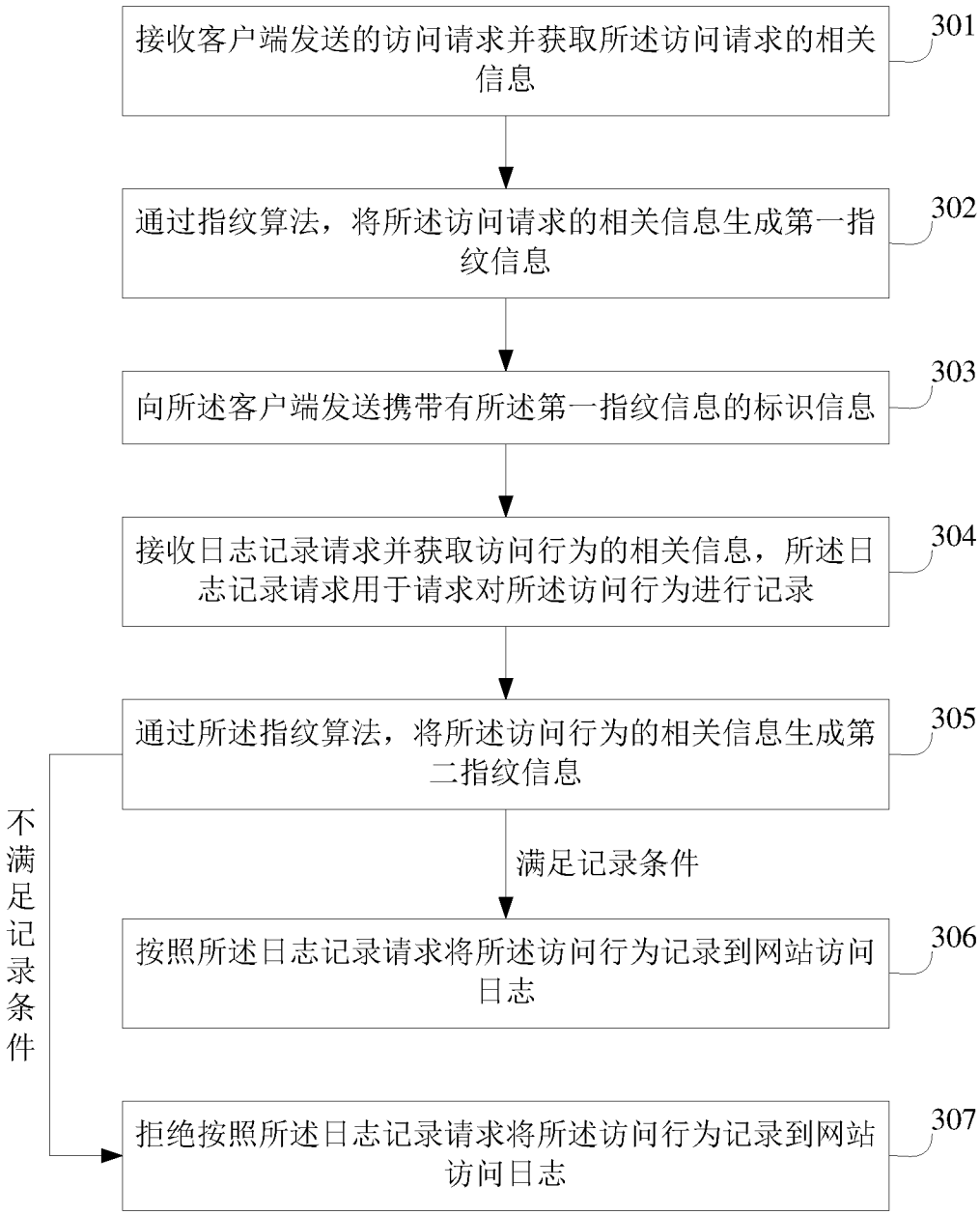

接收客户端发送的访问请求并获取所述访问请求的相关信息
301
通过指纹算法，将所述访问请求的相关信息生成第一指纹信息
302
向所述客户端发送携带有所述第一指纹信息的标识信息
303
接收日志记录请求并获取访问行为的相关信息，所述日志记录请求用于请求对所述访问行为进行记录
304
通过所述指纹算法，将所述访问行为的相关信息生成第二指纹信息
305
满足记录条件
不满足记录条件
按照所述日志记录请求将所述访问行为记录到网站访问日志
306
拒绝按照所述日志记录请求将所述访问行为记录到网站访问日志
307

图 3

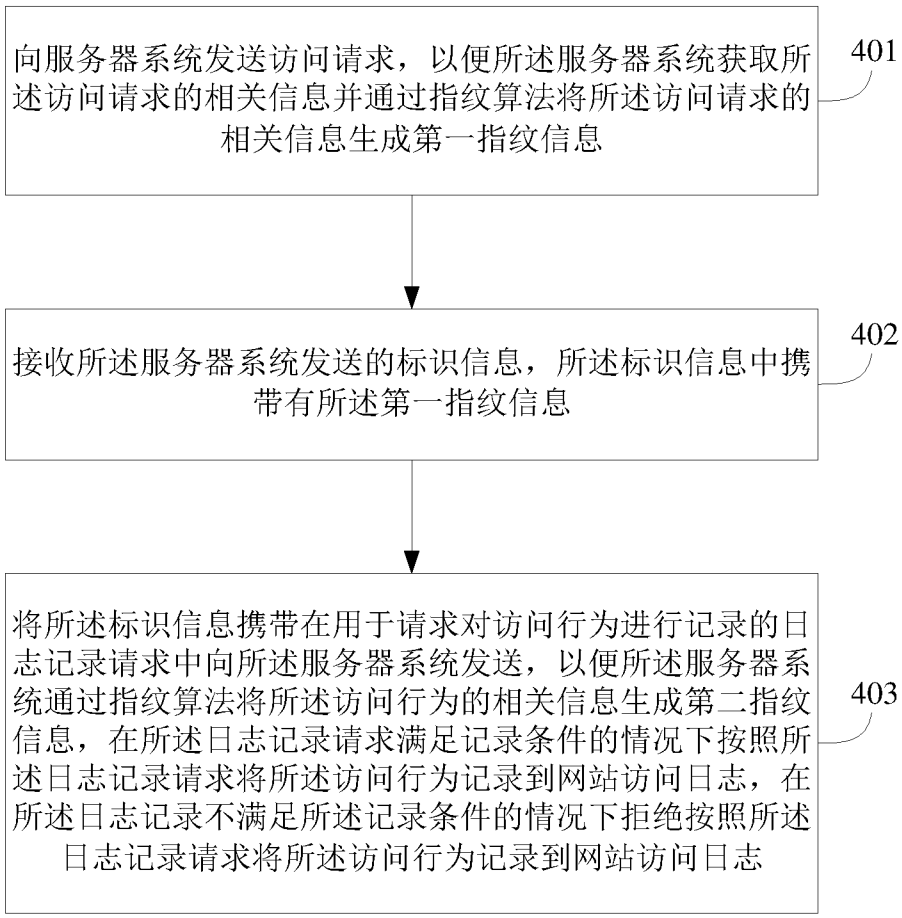

向服务器系统发送访问请求，以便所述服务器系统获取所述访问请求的相关信息并通过指纹算法将所述访问请求的相关信息生成第一指纹信息
401
接收所述服务器系统发送的标识信息，所述标识信息中携带有所述第一指纹信息
402
将所述标识信息携带在用于请求对访问行为进行记录的日志记录请求中向所述服务器系统发送，以便所述服务器系统通过指纹算法将所述访问行为的相关信息生成第二指纹信息，在所述日志记录请求满足记录条件的情况下按照所述日志记录请求将所述访问行为记录到网站访问日志，在所述日志记录不满足所述记录条件的情况下拒绝按照所述日志记录请求将所述访问行为记录到网站访问日志
403

图 4

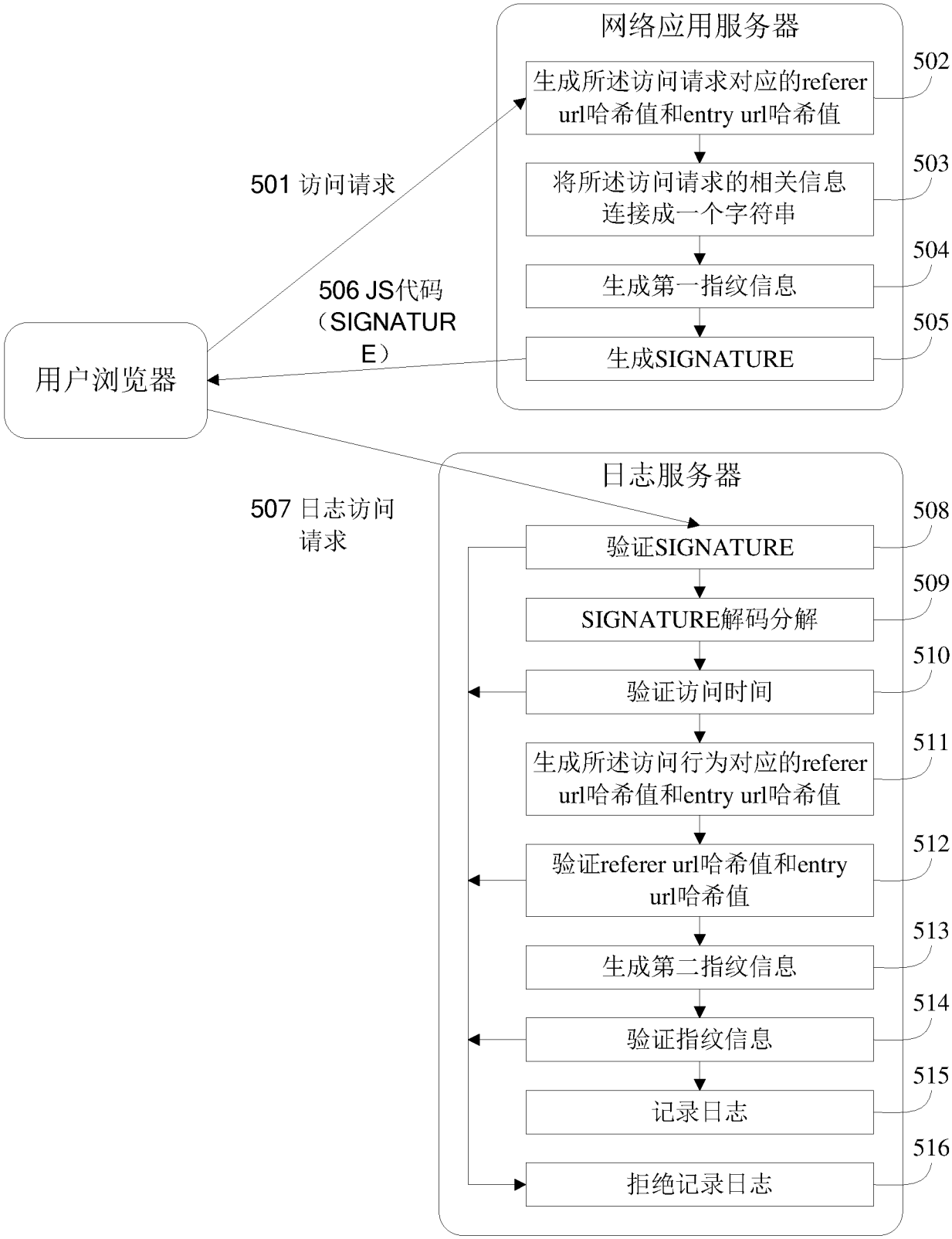

网络应用服务器
生成所述访问请求对应的referer url哈希值和entry url哈希值
502
将所述访问请求的相关信息连接成一个字符串
503
生成第一指纹信息
504
生成SIGNATURE
505
501 访问请求
506 JS代码（SIGNATURE）
用户浏览器
507 日志访问请求
日志服务器
验证SIGNATURE
508
SIGNATURE解码分解
509
验证访问时间
510
生成所述访问行为对应的referer url哈希值和entry url哈希值
511
验证referer url哈希值和entry url哈希值
512
生成第二指纹信息
513
验证指纹信息
514
记录日志
515
拒绝记录日志
516

图 5

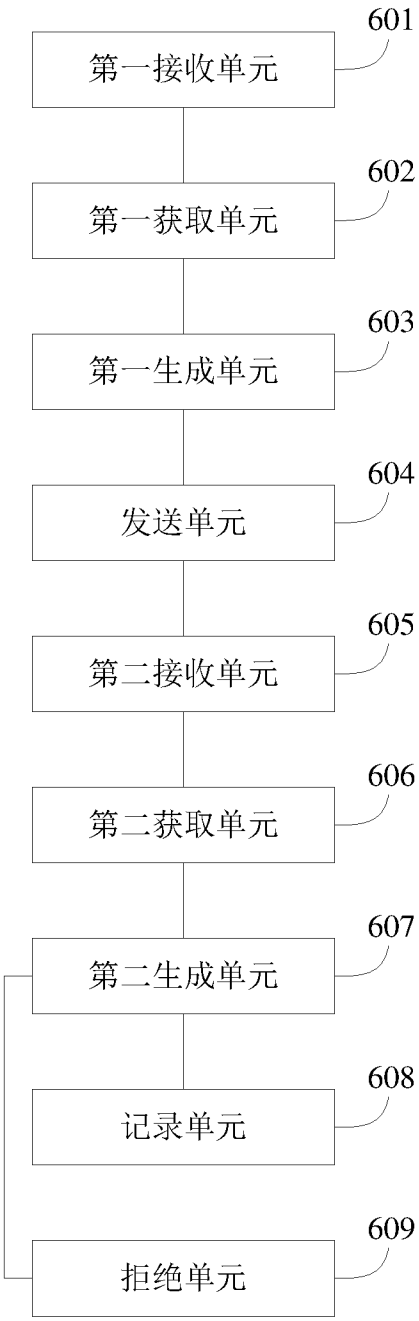

601
第一接收单元
602
第一获取单元
603
第一生成单元
604
发送单元
605
第二接收单元
606
第二获取单元
607
第二生成单元
608
记录单元
609
拒绝单元

图 6

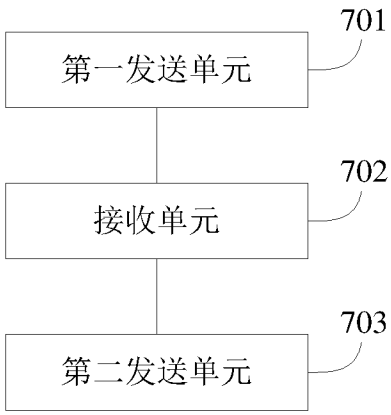


图 7

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2018/077965

A. CLASSIFICATION OF SUBJECT MATTER

H04L 12/24 (2006.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L; G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CPRSABS; CNTXT; VEN; CNKI: 记录, 网站, 网页, 访问日志, 日志记录, 服务器, 客户端, 指纹, 标识, IP 地址, record, web, website, access log, log record, server, client, ID, IP address

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 104765883 A (CEPO (BEIJING) INFORMATION TECHNOLOGY CO., LTD.) 08 July 2015 (08.07.2015), entire document	1-20
A	CN 105721427 A (HUNAN UNIVERSITY) 29 June 2016 (29.06.2016), entire document	1-20
A	CN 104468477 A (HANGZHOU DPTECH TECHNOLOGIES CO., LTD.) 25 March 2015 (25.03.2015), entire document	1-20

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&"document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
23 April 2018	28 April 2018

Name and mailing address of the ISA
State Intellectual Property Office of the P. R. China
No. 6, Xitucheng Road, Jimenqiao
Haidian District, Beijing 100088, China
Facsimile No. (86-10) 62019451

Authorized officer
XU, Gang
Telephone No. (86-10) 62411238

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2018/077965

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 104765883 A	08 July 2015	None	
CN 105721427 A	29 June 2016	None	
CN 104468477 A	25 March 2015	None	

国际检索报告

国际申请号
PCT/CN2018/077965

A. 主题的分类

H04L 12/24(2006.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

H04L; G06F

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用））

CPRSABS;CNTXT;VEN;CNKI:记录，网站，网页，访问日志，日志记录，服务器，客户端，指纹，标识，IP地址，record，web，website，access log，log record，server，client，ID，IP address

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
A	CN 104765883 A (中电运行北京信息技术有限公司) 2015年 7月 8日 (2015-07-08) 全文	1-20
A	CN 105721427 A (湖南大学) 2016年 6月 29日 (2016-06-29) 全文	1-20
A	CN 104468477 A (杭州迪普科技有限公司) 2015年 3月 25日 (2015-03-25) 全文	1-20

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2018年 4月 23日	2018年 4月 28日
ISA/CN的名称和邮寄地址 中华人民共和国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10)62019451	受权官员 徐刚 电话号码 86-(010)-62411238

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2018/077965

检索报告引用的专利文件	公布日（年/月/日）	同族专利	公布日（年/月/日）
CN 104765883 A	2015年 7月 8日	无	
CN 105721427 A	2016年 6月 29日	无	
CN 104468477 A	2015年 3月 25日	无	