(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 103986735 B
(45)授权公告日 2017.04.19

(21)申请号 201410247885.5

(22)申请日 2014.06.05

(65)同一申请的已公布的文献号
申请公布号 CN 103986735 A

(43)申请公布日 2014.08.13

(73)专利权人 北京赛维安讯科技发展有限公司
地址 100085 北京市海淀区清河安宁庄路4号9号办公楼218室

(72)发明人 王斌忠 支小牧 肖毅 岳彩立

(74)专利代理机构 北京思睿峰知识产权代理有限公司 11396
代理人 靳春鹰 赵爱军

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

(56)对比文件
CN 101064729 A,2007.10.31,
CN 101815060 A,2010.08.25,
CN 102263828 A,2011.11.30,
CN 103067409 A,2013.04.24,
CN 101039329 A,2007.09.19,
US 2005198250 A1,2005.09.08,

审查员 蔡红

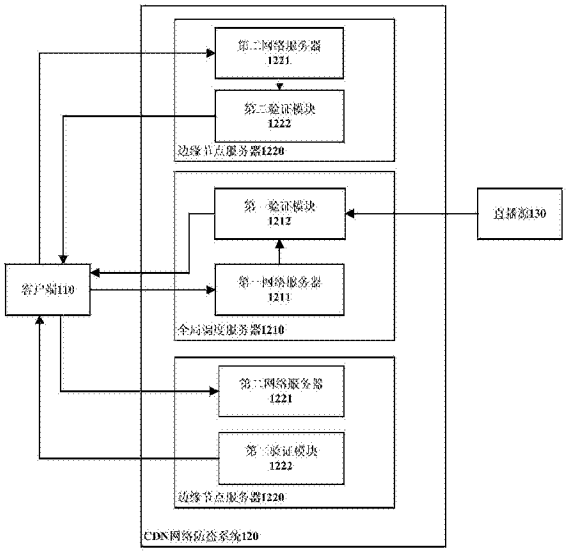
权利要求书3页 说明书10页 附图2页

(54)发明名称

CDN网络防盗系统及防盗方法

(57)摘要

本发明公开了一种CDN网络防盗系统，包括：全局调度服务器，适于接收来自客户端的第一请求，对该第一请求进行验证，根据验证通过的请求生成第二请求，并且将第二请求返回到客户端；和边缘节点服务器，适于接收来自客户端的第二请求，并对该第二请求进行验证，当第二请求验证通过时，返回所述要获取的数据给所述客户端，否则向所述客户端发送验证失败的信息。另外，本发明还提供一种CDN网络防盗方法。利用本发明，解决了多客户、防盗链策略经常变化的直播流防盗链问题，降低了多客户采取不同的防盗链策略和防盗链策略经常变化时的系统实现复杂性和维护成本。



CN 103986735 B

1.一种CDN网络防盗系统，包括全局调度服务器和多个边缘节点服务器，其中，

所述全局调度服务器，适于接收来自客户端的第一请求，对该第一请求进行验证，根据验证通过的请求生成第二请求，并且将第二请求返回到客户端，其中第一请求包括要获取的数据信息，第二请求包括指定多个边缘节点服务器之一的信息以及所述要获取的数据信息；

所述边缘节点服务器，适于接收来自客户端的第二请求，并对该第二请求进行验证，当第二请求验证通过时，返回所述要获取的数据给所述客户端，否则向所述客户端发送验证失败的信息；

其中，所述第一请求包括资源公开识别码、签名串、失效时间戳、标记、客户识别号、和防盗链策略版本号参数。

2.根据权利要求1所述的系统，其中，

所述全局调度服务器包括第一网络服务器和第一验证模块；其中，

所述第一网络服务器接收来自所述客户端的第一请求并将其传送给所述第一验证模块，

所述第一验证模块对来自所述客户端的第一请求进行验证，生成第一验证结果，并将所述第一验证结果发送给所述第一网络服务器；所述第一验证结果包括验证通过和验证失败；

如果所述第一验证结果是验证通过，则所述第一网络服务器生成第二请求，并将第二请求返回到所述客户端；如果第一验证结果是验证失败，则发送验证失败信息给所述第一网络服务器，拒绝所述客户端的请求。

3.根据权利要求1所述的系统，其中，

所述边缘节点服务器包括第二网络服务器和第二验证模块，

所述第二网络服务器接收来自所述客户端的第二请求，并将传送给所述第二验证模块；

所述第二验证模块解析所述第二请求，并对其进行验证，生成第二验证结果，将所述第二验证结果发送给所述第二网络服务器，所述第二验证结果包括验证通过和验证失败；

当所述第二验证结果是验证通过时，所述第二网络服务器将所述客户端要获取的数据发送给所述客户端；

当所述验证结果是验证失败时，所述第二网络服务器将验证失败信息发送给所述客户端，拒绝所述客户端的请求。

4.根据权利要求2所述的系统，其中，

所述第一验证模块对所述客户端的第一请求进行的验证包括如下逻辑验证中的一个或多个：

获取所述客户端请求URL中HTTP请求头中携带的Referer信息，通过判断Referer是否在许可范围中来判断所述请求URL是否为盗链；

获取所述客户端请求URL中HTTP请求头中携带的用户代理User-agent信息，通过判断用户代理User-agent中是否包含特定字符来判断所述请求URL是否为盗链；

将所述客户端的请求URL中携带的失效时间戳与当前时间进行比对，判断所述请求URL是否过期；

根据所述客户识别号和所述防盗链策略版本号参数选取验证密钥对，根据所述验证密钥对和所述客户端的请求URL中的通用唯一识别码、失效时间戳、标记、客户识别号、和版本号参数计算签名串，比较所述客户端的请求URL中的签名串与所述计算得到的签名串是否一致；

根据预先确定的对于不同的客户端设置的禁用或许可规则，判断所述客户端请求URL中的IP是否在禁用或许可范围内；以及

记录相同URL的访问次数，如果相同URL访问两次以上，则判断所述请求URL为盗链。

5.根据权利要求1－4中任何一项所述的系统，其中，

所述第二请求中的所述指定多个边缘节点服务器之一的信息包括：

资源编号sid，其与通用唯一识别码一一对应，从所述通用唯一识别码解密后获取；

失效时间戳tm；以及

链接校验参数k，其根据资源编号sid、失效时间戳tm和密钥进行不可逆哈希计算后得到的字符串。

6.根据权利要求5所述的系统，其中，

所述第二验证模块对所述客户端的第二请求所进行的验证包括如下逻辑验证中的一个或者多个：

比较所述客户端的第二请求中包含的URL中携带的失效时间戳与当前时间的大小，如果所述失效时间戳在当前时间之前，则所述客户端的请求URL失效，否则有效；

通过判断链接校验参数k值是否变化来判断所述客户端的第二请求中包含的URL是否被篡改；

获取发出第一请求的客户端的IP地址，判断该第一请求是否为首次请求，如果是首次请求，则记录所述客户端的对应的IP段；如果是非首次请求，验证和首次请求的IP段是否一致，不一致则认为所述客户端的请求是盗链请求。

7.一种CDN网络防盗方法，包括：

接收客户端发送的要获取数据信息的第一请求，其中，第一请求包括要获取的数据信息；

对该第一请求进行验证，生成第一验证结果，其中第一验证结果包括验证通过和验证失败；

判断所述第一验证结果是否是验证通过，当第一验证结果为验证失败时，向客户端发送请求失败的信息；当第一验证结果为验证通过时，生成第二请求，并将第二请求发送给所述客户端；其中，第二请求包括指定多个边缘节点服务器之一的信息以及所述要获取的数据信息；

所述边缘节点服务器接收所述客户端发送的第二请求；

所述边缘节点服务器对该第二请求进行验证，生成第二验证结果，其中第二验证结果包括验证通过和验证失败；以及

判断所述第二验证结果是否是验证通过，当第二验证结果为验证失败时，向客户端发送请求失败的信息；当第二验证结果为验证通过时，将所述客户端要获取的数据信息发送给所述客户端；

其中，所述第一请求包括通用唯一识别码、签名串、失效时间戳、标记、客户识别号、和

防盗链策略版本号参数。

8.根据权利要求7所述的方法，其中，

所述对第一请求进行的验证包括如下逻辑验证中的一个或多个：

获取所述客户端请求URL中HTTP请求头中携带的REFERER信息，通过判断REFERER是否在许可范围中来判断所述请求URL是否为盗链；

获取所述客户端请求URL中HTTP请求头中携带的用户代理user-agent信息，通过判断用户代理user-agent中是否包含特定字符来判断所述请求URL是否为盗链；

将所述客户端的请求URL中携带的失效时间戳与当前时间进行比对，判断所述请求URL是否过期；

根据所述客户识别号和所述防盗链策略版本号参数选取验证密钥对，根据所述验证密钥对和所述客户端的请求URL中的通用唯一识别码、失效时间戳、标记、客户识别号、和版本号参数计算签名串，比较所述客户端的请求URL中的签名串与所述计算得到的签名串是否一致；

根据预先确定的对于不同的客户端设置的禁用或许可规则，判断所述客户端请求URL中的IP是否在禁用或许可范围内；以及

记录相同URL的访问次数，如果相同URL访问两次以上，则判断所述请求URL为盗链。

9.根据权利要求7或8所述的方法，其中，

所述第二请求中的所述指定多个边缘节点服务器之一的信息包括：

资源编号sid，其与通用唯一识别码一一对应，从所述通用唯一识别码解密后获取；

失效时间戳tm；以及

链接校验参数k，其根据资源编号sid、失效时间戳tm和密钥进行不可逆哈希计算后得到的字符串。

10.根据权利要求9所述的方法，其中，

所述对第二请求进行的验证包括如下逻辑验证中的一个或者多个：

比较所述客户端的第二请求中包含的URL中携带的失效时间戳与当前时间的大小，如果所述失效时间戳在当前时间之前，则所述客户端的请求URL失效，否则有效；

通过判断链接校验参数k值是否变化来判断所述客户端的第二请求中包含的URL是否被篡改；

获取发出第一请求的客户端的IP地址，判断该第一请求是否为首次请求，如果是首次请求，则记录所述客户端的第一请求中URL对应的IP段；如果是非首次请求，验证和首次请求的IP段是否一致，不一致则认为所述客户端的请求是盗链请求。

CDN网络防盗系统及防盗方法

技术领域

[0001] 本发明涉及互联网技术领域，尤其涉及CDN网络防盗系统及防盗方法。

背景技术

[0002] 一般地，当用户浏览页面时，一个完整的页面并不是一次全部传送到客户端。一个网站中如果没有其页面中所说的信息，例如图片信息，那么它完全可以将这个图片链接到别的网站。这样没有任何资源的网站利用了别的网站的资源来展示给浏览者，提高了自己的访问量，而大部分浏览者又不会很容易地发现，这样显然，对于那个被利用了资源的网站是不公平的。一些不良网站为了不增加成本而扩充自己站点内容，经常盗用其他网站的链接。一方面损害了原网站的合法利益，另一方面又加重了服务器的负担。因此，相应地产生了防盗链技术。

[0003] 防盗链的实现原理是，在HTTP协议中，有一个表头字段叫referer，采用URL的格式来表示从哪儿链接到当前的网页或文件。换句话说，通过referer，网站可以检测目标网页访问的来源网页，如果是资源文件，则可以跟踪到显示它的网页地址。有了referer跟踪来源，就可以通过技术手段来进行处理，一旦检测到来源不是本站即进行阻止或者返回指定的页面。

[0004] 目前防盗链策略有多种，例如，基于时间的防盗链会携带失效时间戳变量，然后验证失效时间戳是否在有效范围内；基于IP的防盗链会先携带用户IP地址，然后验证访问IP和携带的IP两个参数是否一致。

[0005] 播放源的数据在经过对于CDN网络分发系统，一般整个系统采用一种防盗链策略，多种防盗链策略不能并存，防盗链策略升级影响范围较大，升级可能导致客户灾难性后果。但是，CDN分发系统的防盗链不同于其他领域的防盗链，CDN分发系统的防盗链一般有一定的客户量，每个客户可能采取不同的防盗链策略，另外，客户的防盗链策略还会经常周期性变化。因此，目前的CDN分发系统的防盗链不能适应多客户、以及防盗链策略经常改变的应用场景。另外，当用户有多个出口IP时，携带的IP和验证模块获取的IP地址可能不一致，会导致误判。

发明内容

[0006] 鉴于上述问题，提出了本发明以便提供一种克服上述问题或者至少部分地解决上述问题的CDN网络防盗系统及防盗方法。

[0007] 依据本发明的一个方面，提供了一种CDN网络防盗系统，包括全局调度服务器和多个边缘节点服务器。其中，所述全局调度服务器，适于接收来自客户端的第一请求，对该第一请求进行验证，根据验证通过的请求生成第二请求，并且将第二请求返回到客户端，其中第一请求包括要获取的数据信息，第二请求包括指定多个边缘节点服务器之一的信息以及所述要获取的数据信息。所述边缘节点服务器，适于接收来自客户端的第二请求，并对该第二请求进行验证，当第二请求验证通过时，返回所述要获取的数据给所述客户端，否则向所

述客户端发送验证失败的信息。

[0008] 根据本发明上述的CDN网络防盗系统，所述全局调度服务器包括第一网络服务器和第一验证模块；其中，所述第一网络服务器接收来自所述客户端的第一请求并将其传送给所述第一验证模块。所述第一验证模块对来自所述客户端的第一请求进行验证，生成第一验证结果，并将所述第一验证结果发送给所述第一网络服务器；所述第一验证结果包括验证通过和验证失败。如果所述第一验证结果是验证通过，则所述第一网络服务器生成第二请求，并将第二请求返回到所述客户端；如果第一验证结果是验证失败，则发送验证失败信息给所述第一网络服务器，拒绝所述客户端的请求。

[0009] 根据本发明上述的CDN网络防盗系统，所述边缘节点服务器包括第二网络服务器和第二验证模块。所述第二网络服务器接收来自所述客户端的第二请求，并将传送给所述第二验证模块；所述第二验证模块解析所述第二请求，并对其进行验证，生成第二验证结果，将所述第二验证结果发送给所述第二网络服务器，所述第二验证结果包括验证通过和验证失败；当所述第二验证结果是验证通过时，所述第二网络服务器将所述客户端要获取的数据发送给所述客户端；当所述验证结果是验证失败时，所述第二网络服务器将验证失败信息发送给所述客户端，拒绝所述客户端的请求。

[0010] 依据本发明的另一个方面，提供了一种CDN网络防盗方法，包括：接收客户端发送的要获取数据信息的第一请求，其中，第一请求包括要获取的数据信息；对该第一请求进行验证，生成第一验证结果，其中第一验证结果包括验证通过和验证失败；判断所述第一验证结果是否是验证通过，当第一验证结果为验证失败时，向客户端发送请求失败的信息；当第一验证结果为验证通过时，生成第二请求，并将第二请求发送给所述客户端；其中，第二请求包括指定多个边缘节点服务器之一的信息以及所述要获取的数据信息；所述边缘节点服务器接收所述客户端发送的第二请求；所述边缘节点服务器对该第二请求进行验证，生成第二验证结果，其中第二验证结果包括验证通过和验证失败；以及判断所述第二验证结果是否是验证通过，当第二验证结果为验证失败时，向客户端发送请求失败的信息；当第二验证结果为验证通过时，将所述客户端要获取的数据信息发送给所述客户端。

[0011] 利用本发明，解决了多客户、防盗链策略经常变化的直播流防盗链问题，降低了多客户采取不同的防盗链策略和防盗链策略经常变化时的系统实现复杂性和维护成本。

[0012] 上述说明仅是本发明技术方案的概述，为了能够更清楚了解本发明的技术手段，而可依照说明书的内容予以实施，并且为了让本发明的上述和其它目的、特征和优点能够更明显易懂，以下特举本发明的具体实施方式。

附图说明

[0013] 通过阅读下文优选实施方式的详细描述，各种其他的优点和益处对于本领域普通技术人员将变得清楚明了。附图仅用于示出优选实施方式的目的，而并不认为是对本发明的限制。而且在整个附图中，用相同的参考符号表示相同的部件。在附图中：

[0014] 图1示出了根据本发明的一种实施方式的CDN网络防盗系统的结构示意图；以及

[0015] 图2示出了根据本发明的一个实施方式的CDN网络防盗方法的流程图。

具体实施方式

[0016] 下面将参照附图更详细地描述本公开的示例性实施例。虽然附图中显示了本公开的示例性实施例，然而应当理解，可以以各种形式实现本公开而不应被这里阐述的实施例所限制。相反，提供这些实施例是为了能够更透彻地理解本公开，并且能够将本公开的范围完整的传达给本领域的技术人员。

[0017] 在当前的使用CDN网络分发数据的互联网系统中，例如基于CDN网络将直播源的直播数据提供给向直播源请求直播数据的客户端。在这些客户端中，可能存在盗用直播数据的盗链情形。为此，在CDN网络中设置本发明的CDN网络防盗系统。

[0018] 图1示出了根据本发明的一种实施方式的CDN网络防盗系统的结构示意图。如图1所示，本发明的CDN网络防盗系统120包括全局调度服务器1210和多个边缘节点服务器1220。

[0019] 全局调度服务器1210本身不提供服务，主要用于调度各边缘节点服务器1220。具体地，全局调度服务器1210接收来自客户端110的第一请求，对该第一请求进行验证，在验证通过时生成第二请求，并且将第二请求返回到客户端110。

[0020] 其中第一请求是加过密的URL或者是有防盗链的URL。URL的加密通过与厂家协商确定，通常由厂家提供一个加密密钥，来实现URL的加密。

[0021] 第一请求包括要获取的数据信息(例如要获取的数据的网址)以及如下各项中的一项或者多项：

[0022] uuid:代表资源公开识别码(或称资源公开ID)，是通用唯一识别码(Universally Unique Identifier)，其中包含了资源的一些信息，如内部编号等，采用可逆加密处理，避免系统信息泄露；

[0023] sign:验证串(即签名串)，是为了做防盗链验证，避免第一请求地址被篡改；

[0024] timestamp:失效时间戳tm，用来检查第一请求地址是否在有效时间之内；

[0025] ai:即app id(即客户编号)，也称为客户识别(ID)号，对应一个客户，例如一个公司或者组织，用于区分不同的客户；

[0026] v:防盗链策略版本号。各版本有不同特性，可各自独立使用，便于用户平滑升级。

[0027] flag:是开关变量，可实现开关。例如:是否禁用防盗链，标识为d。需禁用防盗链时则为“d”，不禁用防盗链时则为空，满足某些特定场合使用。

[0028] 例如，第一请求可以为如下格式：

[0029] http://<domain>/?uuid＝{uuid}

[0030] & sign＝{sign}

[0031] &timestamp＝{timestamp}

[0032] &flag＝{flag}

[0033] &ai＝{app id}

[0034] &v＝{version}

[0035] 第二请求包括指定多个边缘节点服务器1220之一的信息以及所述要获取的数据信息。所述指定多个边缘节点服务器1220之一的信息包括客户端的第一请求中的一些信息以及指向被指定的边缘节点服务器1220的URL地址。例如，第二请求中的所述指定多个边缘节点服务器之一的信息可以包括如下信息：

[0036] 资源编号sid(source ID):其与资源公开ID(uuid)一一对应，从所述资源公开ID

解密后获取；

[0037] 失效时间戳tm；timestamp，用来检查第一请求地址是否在有效时间之内；以及

[0038] 链接校验参数k：是用来判断第二请求地址是否被篡改，其根据资源编号sid、失效时间戳tm和密钥key(这里的key是和客户约定的)进行不可逆哈希计算后得到的字符串，即，k＝hash(<sid>+<timestamp>+<key>)，例如K为通过上述计算后得到的32位字符串。

[0039] 例如，第二请求可以为如下格式：

[0040] http://<domain>/?sid＝{sid}&tm＝{tm}&k＝{k}

[0041] 进一步地，全局调度服务器1210可以包括第一网络服务器1211和第一验证模块1212。

[0042] 其中，第一网络服务器1211接收来自客户端110的第一请求并将其传送给第一验证模块1212。例如，客户端110将包含要获取的信息的请求URL发送给第一验证模块1212。

[0043] 第一验证模块1212对来自客户端110的第一请求进行验证，生成第一验证结果，并将所述第一验证结果发送给第一网络服务器1211。第一验证结果包括验证通过和验证失败。

[0044] 第一验证模块1212在接收到来自客户端110的第一请求后，首先，对该第一请求进行防盗链验证。如果验证未通过，则对第一请求的请求URL不进行处理，向第一网络服务器1211发送验证失败的信息，第一网络服务器1211向客户端110发送“请求失败”的信息，拒绝客户端110的获取数据的请求。如果验证通过，则发送验证成功的信息给第一网络服务器1211，第一网络服务器1211基于验证通过的信息而生成第二请求，并将第二请求返回给客户端110。

[0045] 第一验证模块1212引入了客户ID和防盗链策略版本号参数，通过客户ID和防盗链策略版本号参数的组合，使得本发明可以适配不同客户、不同的直播防盗链策略需求。

[0046] 第一验证模块1212对客户端110的第一请求进行的验证可以包括如下逻辑验证中的一个或多个：

[0047] 1)获取客户端110第一请求中的HTTP请求头中携带的Referer信息，通常，每个ai(即，客户识别号，对应一个客户，例如一个公司或者组织)对应一个referer列表。通过判断Referer是否在许可范围中来判断所述第一请求中的请求URL是否为盗链。如果判断Referer不在许可范围内，则判断该请求URL为盗链，向客户端返回HTTP412，拒绝该客户端的请求。

[0048] Referer是HTTP协议的请求头的一部分，当客户端浏览器向web服务器发送请求的时候，一般会带上Referer，告诉服务器客户端是从哪个页面链接过来的，服务器由此可以获得一些信息用于处理。比如，从我主页上链接到一个朋友那里，他的服务器就能够从Referer中统计出每天有多少用户点击我主页上的链接访问他的网站。

[0049] 2)获取客户端110第一请求中的HTTP请求头中携带的用户代理User-agent信息，通过判断用户代理User-agent中是否包含特定字符来判断所述第一请求中的请求URL是否为盗链。所述特定字符例如SOONER字符串。

[0050] 这里，用户代理User-Agent是Http协议中的一部分，属于请求头的组成部分，其是一种向访问网站提供用户所使用的浏览器类型、操作系统及版本、CPU类型、浏览器渲染引擎、浏览器语言、浏览器插件等信息的标识。

[0051] 3)将客户端110的第一请求中携带的失效时间戳tm(timestamp)与当前时间进行比对,判断客户端的请求URL是否过期,失效时间戳tm为0则没有过期,如果过期(即tm早于当前时间,不为零)则返回HTTP412,判定所述第一请求中的请求URL为盗链,拒绝该客户端的请求。

[0052] 4)根据所述客户ID号(即ai或app id)和所述防盗链策略版本号参数v选取验证密钥对key(ai和v的组合与key有个对应关系),根据所述验证密钥对key和所述客户端的请求URL中的资源公开ID、失效时间戳、标记、客户ID号、和版本号参数计算签名串calsign,calsign的计算方法为:

[0053] <calsign>=md5(<appid>+<key>+<timestamp>+<uuid>+<flag>+<version>+<自定义的传入参数>

[0054] 其中,自定义的传入参数通过是在URL中增加的,这里只是从URL中将其取出。比较所述客户端的请求URL中的签名串sign与所述计算得到的签名串calsign是否一致。如果一致,则验证通过客户端的请求;否则拒绝客户端的请求,向客户端返回HTTP412。

[0055] 5)针对于不同的客户端(用ai表示),设置相应的禁用或许可规则,根据所设置的禁用或许可规则来判断所述客户端的IP是否在禁用或许可范围内,从而达到限定IP的访问请求的目的。

[0056] 其中,通过参数<flag>设置开关处理逻辑disable,设置是否禁用防盗链。标识为d。如果禁用防盗链,则<flag>为“d”,如果不禁用防盗链,则<flag>为为空,这满足某些特定场合使用。值得注意的是,当进行禁用防盗链判断时,最好同时将失效时间戳tm(timestamp)设为0,否则可能会因为先行判断失效时间戳tm失效(即过期)导致客户端的请求被拒绝。

[0057] 6)记录相同请求URL的访问次数,如果相同请求URL访问两次以上,则判断所述请求URL为盗链,则拒绝该客户端的请求,向客户端返回HTTP412,由此,可以达到限定用户的目的。

[0058] 第一验证模块1212对客户端110的第一请求进行验证时,可以选用上述逻辑验证规则中的一个或多个,通常会选用第1)、3)、5)和6)条逻辑验证规则。

[0059] 以上只是示例性列出了第一验证模块1212对客户端110的第一请求进行验证的几条逻辑验证规则,本发明并不限于上述逻辑验证规则,也可以包含更多的逻辑验证规则。

[0060] 如果第一验证模块1212的验证结果为验证通过,则将验证通过的验证结果发送给第一网络服务器1211。第一网络服务器1211基于验证通过的信息,为所述客户端分配一个边缘节点服务器1220,并生成第二请求,将第二请求以HTTP302的方式返回给客户端110。如前所述,第二请求中包含被分配的边缘节点服务器1220的URL,以便客户端能根据所述URL向该被分配的边缘节点服务器1220发送请求。

[0061] 边缘节点服务器1220适于接收来自客户端110的第二请求,并对该第二请求进行验证,当第二请求验证通过时,返回所述要获取的数据给客户端110,否则向客户端110发送验证失败的信息。

[0062] 具体地,边缘节点服务器1220可以包括第二网络服务器1221和第二验证模块1222。其中,第二网络服务器1221接收来自客户端110的第二请求,并将传送给第二验证模块1222。第二验证模块1222解析所述第二请求,并对其进行验证,生成第二验证结果,将所

述第二验证结果发送给第二网络服务器1221，所述第二验证结果包括验证通过和验证失败。

[0063] 当所述第二验证结果是验证通过时，第二网络服务器1221将所述客户端110要获取的数据发送给所述客户端110。

[0064] 当所述验证结果是验证失败时，第二网络服务器1221向所述客户端110发送“请求失败”的信息，拒绝客户端110的请求。

[0065] 其中，第二验证模块1222解析所述第二请求，通过如下的逻辑验证以对请求URL进行防盗链验证：

[0066] 1)请求URL是否在有效期的验证：

[0067] 对于合法用户来说，获取的第二请求并不是可以永远无限制的使用。第二请求中携带有失效时间戳tm。第二验证模块会比较失效时间戳tm与当前时间的大小，如果所述失效时间戳tm在当前时间之前，则该第二请求失效，否则有效；

[0068] 2)URL唯一性验证

[0069] 用户的第二请求中包括资源编号sid和精确到毫秒的失效时间戳tm。失效时间戳tm的产生和服务器的系统时间以及同一时间的请求数量有关。由于不同请求产生的相同链接的几率非常小，所以可以认为第二请求是唯一的。通过判断链接校验参数k值是否变化，可以判断第二请求是否被篡改。k值的计算方法如前面所述。

[0070] 3)请求IP段验证

[0071] 获取用户发出第一请求时的IP地址，判断该第一请求是否为首次请求，如果是首次请求，则记录用户的第一请求对应的IP段；如果是非首次请求，则验证和首次请求的IP段是否一致，不一致则认为所述用户的第一请求是盗链请求。另外，记录首次请求时和IP段对应的数据，在首次请求过期后自动消除。

[0072] 通常，第二验证模块1222在对请求URL进行防盗链验证时，进行上述三项逻辑验证。

[0073] 本发明还提供一种CDN网络防盗方法，如图2所示，本发明的CDN网络防盗方法200起始于步骤S210，在步骤S210，接收客户端发送的要获取数据信息的第一请求。

[0074] 这里，其中第一请求是加过密的URL或者是有防盗链的URL。URL的加密通过与厂家协商确定，通常由厂家提供一个加密密钥，来实现URL的加密。

[0075] 第一请求包括要获取的数据信息(例如要获取的数据的网址)以及如下各项中的一项或者多项：

[0076] uuid：资源公开ID，是通用唯一识别码(Universally Unique Identifier)；

[0077] sign：验证串(即签名串)；

[0078] timestamp：失效时间戳tm；

[0079] ai：app id(即客户编号)，也称为客户识别(ID)号；

[0080] v：防盗链策略版本号，各版本有不同特性，可各自独立使用，便于用户平滑升级。

[0081] flag：是开关变量，可实现开关。例如：是否禁用防盗链，标识为d。需禁用防盗链时则为“d”，不禁用防盗链时则为空，满足某些特定场合使用。

[0082] 例如，第一请求可以为如下格式：

[0083] http://<domain>/?uuid＝{uuid}

[0084] & sign＝{sign}

[0085] &timestamp＝{timestamp}

[0086] &flag＝{flag}

[0087] &ai＝{app id}

[0088] &v＝{version}

[0089] 接下来，执行步骤S220，对所述第一请求进行验证，生成第一验证结果。第一验证结果包括验证通过和验证失败。

[0090] 对所述第一请求进行验证主要采用如下的一个或多个逻辑验证：

[0091] 1)获取第一请求中的HTTP请求头中携带的Referer信息。通过判断Referer是否在许可范围中来判断所述第一请求中的请求URL是否为盗链。如果判断Referer不在许可范围内，则判断该请求URL为盗链，向客户端返回HTTP412，拒绝该客户端的请求。

[0092] 2)获取客户端110第一请求中的HTTP请求头中携带的用户代理User-agent信息，通过判断用户代理User-agent中是否包含特定字符来判断所述第一请求中的请求URL是否为盗链。所述特定字符例如SOONER字符串。

[0093] 3)将客户端110的第一请求中携带的失效时间戳tm(timestamp)与当前时间进行比对，判断客户端的请求URL是否过期，失效时间戳tm为0则没有过期，如果过期(即tm早于当前时间，不为零)则返回HTTP412，判定所述第一请求中的请求URL为盗链，拒绝该客户端的请求。

[0094] 4)根据所述客户ID号(即ai或app id)和所述防盗链策略版本号参数v选取验证密钥对key(ai和v的组合与key有个对应关系)，根据所述验证密钥对key和所述客户端的请求URL中的资源公开ID、失效时间戳、标记、客户ID号、和版本号参数计算签名串calsign，calsign的计算方法为：

[0095] <calsign>＝md5(<appid>+<key>+<timestamp>+<uuid>+<flag>+<version>+<自定义的传入参数>。

[0096] 其中，自定义的传入参数通过是在URL中增加的，这里只是从URL中将其取出。比较所述客户端的请求URL中的签名串sign与所述计算得到的签名串calsign是否一致。如果一致，则验证通过客户端的请求；否则拒绝客户端的请求，向客户端返回HTTP412。

[0097] 5)针对于不同的客户端(用ai表示)，设置相应的禁用或许可规则，根据所设置的禁用或许可规则来判断所述客户端的IP是否在禁用或许可范围内，从而达到限定IP的访问请求的目的。

[0098] 其中，通过参数<flag>设置开关处理逻辑disable，设置是否禁用防盗链。标识为d。如果禁用防盗链，则<flag>为“d”，如果不禁用防盗链，则<flag>为为空，这满足某些特定场合使用。值得注意的是，当进行禁用防盗链判断时，最好同时将失效时间戳tm(timestamp)设为0，否则可能会因为先行判断失效时间戳tm失效(即过期)导致客户端的请求被拒绝。

[0099] 6)记录相同请求URL的访问次数，如果相同请求URL访问两次以上，则判断所述请求URL为盗链，则拒绝该客户端的请求，向客户端返回HTTP412，由此，可以达到限定用户的目的。

[0100] 以上只是示例性列出了第一验证模块1212对客户端110的第一请求进行验证的几

条逻辑验证规则，本发明并不限于上述逻辑验证规则，也可以包含更多的逻辑验证规则。

[0101] 接下来，执行步骤S230，判断第一验证结果是否为验证通过。当第一验证结果为验证失败时，则执行步骤S240，向客户端发送“请求失败”的信息，例如，向客户端返回HTTP412，拒绝客户端的请求；

[0102] 当第一验证结果为验证通过时，则执行步骤S250，生成第二请求；

[0103] 第二请求包括指定多个边缘节点服务器1220之一的信息以及所述要获取的数据信息。所述指定多个边缘节点服务器1220之一的信息包括客户端的第一请求中的一些信息以及指向被指定的边缘节点服务器1220的URL地址。例如，第二请求中的所述指定多个边缘节点服务器之一的信息可以包括如下信息：

[0104] 资源编号sid：其与资源公开ID(uuid)一一对应，从所述资源公开ID解密后获取；

[0105] 失效时间戳tm；timestamp；以及

[0106] 链接校验参数k：根据资源编号sid、失效时间戳tm和密钥进行不可逆哈希计算后得到的字符串，即，k＝hash(<sid>+<timestamp>+<key>)，例如K为通过上述计算后得到的32位字符串。

[0107] 例如，第二请求可以为如下格式：

[0108] http://<domain>/?sid＝{sid}&tm＝{tm}&k＝{k}

[0109] 接下来，执行步骤S260，将第二请求发送给所述客户端。

[0110] 在步骤S260之后，执行步骤S270，第二请求中被指定的边缘节点服务器接收客户端发送的第二请求。

[0111] 接下来，在步骤S280，所述边缘节点服务器对第二请求进行验证，生成第二验证结果。所述第二验证结果包括验证通过和验证失败。第二验证模块1222解析所述第二请求，通过逐个进行如下逻辑验证以对请求URL进行防盗链验证：

[0112] 1)请求URL是否在有效期的验证：

[0113] 对于合法用户来说，获取的第二请求并不是可以永远无限制的使用。第二请求中携带有失效时间戳tm。第二验证模块会比较失效时间戳tm与当前时间的大小，如果所述失效时间戳tm在当前时间之前，则该链接失效，否则有效；

[0114] 2)URL唯一性验证

[0115] 用户的第二请求中包括资源编号sid和精确到毫秒的失效时间戳tm。失效时间戳tm的产生和服务器的系统时间以及同一时间的请求数量有关。由于不同请求产生的相同链接的几率非常小，所以可以认为第二请求是唯一的。通过判断链接校验参数k值是否变化，可以判断第二请求是否被篡改。k值的计算方法如前面所述。

[0116] 3)请求IP段验证

[0117] 获取用户发出第一请求时的IP地址，判断该第一请求是否为首次请求，如果是首次请求，则记录用户的第一请求对应的IP段；如果是非首次请求，则验证和首次请求的IP段是否一致，不一致则认为所述用户的第一请求是盗链请求。另外，记录首次请求时和IP段对应的数据，在首次请求所记录的IP数据在过期后自动消除。有些情况下，用户的出口IP有多个，所以用户的出口IP可能会变化，这时会出现误判为盗链的情况。

[0118] 接下来，在步骤S290，判断第二验证结果是否为验证通过。当第二验证结果为验证通过时，则执行步骤S291，将客户端所要获取的数据发送给客户端；当第二验证结果为验证

失败时，则执行步骤S292，向客户端发送“请求失败”的信息。

[0119] 本发明利用表示客户ID号的参数ai和防盗链策略版本号的参数v，能够区分每一个客户以及其所使用的防盗链策略，由此解决了不同客户采用不同的防盗链策略或者防盗链策略经常变化的直播流防盗链问题，降低了多客户采取不同的防盗链策略和防盗链策略经常变化时的系统实现复杂性和维护成本。另外，本发明利用IP段的验证逻辑，降低了防盗链误判的几率。

[0120] 在此提供的算法和显示不与任何特定计算机、虚拟系统或者其它设备固有相关。各种通用系统也可以与基于在此的示教一起使用。根据上面的描述，构造这类系统所要求的结构是显而易见的。此外，本发明也不针对任何特定编程语言。应当明白，可以利用各种编程语言实现在此描述的本发明的内容，并且上面对特定语言所做的描述是为了披露本发明的最佳实施方式。

[0121] 在此处所提供的说明书中，说明了大量具体细节。然而，能够理解，本发明的实施例可以在没有这些具体细节的情况下实践。在一些实例中，并未详细示出公知的方法、结构和技术，以便不模糊对本说明书的理解。

[0122] 类似地，应当理解，为了精简本公开并帮助理解各个发明方面中的一个或多个，在上面对本发明的示例性实施例的描述中，本发明的各个特征有时被一起分组到单个实施例、图、或者对其的描述中。然而，并不应将该公开的方法解释成反映如下意图：即所要求保护的本发明要求比在每个权利要求中所明确记载的特征更多的特征。更确切地说，如下面的权利要求书所反映的那样，发明方面在于少于前面公开的单个实施例的所有特征。因此，遵循具体实施方式的权利要求书由此明确地并入该具体实施方式，其中每个权利要求本身都作为本发明的单独实施例。

[0123] 本领域那些技术人员可以理解，可以对实施例中的设备中的模块进行自适应性地改变并且把它们设置在与该实施例不同的一个或多个设备中。可以把实施例中的模块或单元或组件组合成一个模块或单元或组件，以及此外可以把它们分成多个子模块或子单元或子组件。除了这样的特征和/或过程或者单元中的至少一些是相互排斥之外，可以采用任何组合对本说明书(包括伴随的权利要求、摘要和附图)中公开的所有特征以及如此公开的任何方法或者设备的所有过程或单元进行组合。除非另外明确陈述，本说明书(包括伴随的权利要求、摘要和附图)中公开的每个特征可以由提供相同、等同或相似目的的替代特征来代替。

[0124] 此外，本领域的技术人员能够理解，尽管在此所述的一些实施例包括其它实施例中所包括的某些特征而不是其它特征，但是不同实施例的特征的组合意味着处于本发明的范围之内并且形成不同的实施例。例如，在下面的权利要求书中，所要求保护的实施例的任意之一都可以以任意的组合方式来使用。

[0125] 本发明的各个部件实施例可以以硬件实现，或者以在一个或者多个处理器上运行的软件模块实现，或者以它们的组合实现。本领域的技术人员应当理解，可以在实践中使用微处理器或者数字信号处理器(DSP)来实现根据本发明实施例的浏览器客户端中的一些或者全部部件的一些或者全部功能。本发明还可以实现为用于执行这里所描述的方法的一部分或者全部的设备或者装置程序(例如，计算机程序和计算机程序产品)。这样的实现本发明的程序可以存储在计算机可读介质上，或者可以具有一个或者多个信号的形式。这样的

信号可以从因特网网站上下载得到，或者在载体信号上提供，或者以任何其他形式提供。

[0126] 应该注意的是上述实施例对本发明进行说明而不是对本发明进行限制，并且本领域技术人员在不脱离所附权利要求的范围的情况下可设计出替换实施例。在权利要求中，不应将位于括号之间的任何参考符号构造成对权利要求的限制。单词“包含”不排除存在未列在权利要求中的元件或步骤。位于元件之前的单词“一”或“一个”不排除存在多个这样的元件。本发明可以借助于包括有若干不同元件的硬件以及借助于适当编程的计算机来实现。在列举了若干装置的单元权利要求中，这些装置中的若干个可以是通过同一个硬件项来具体体现。单词第一、第二、以及第三等的使用不表示任何顺序。可将这些单词解释为名称。

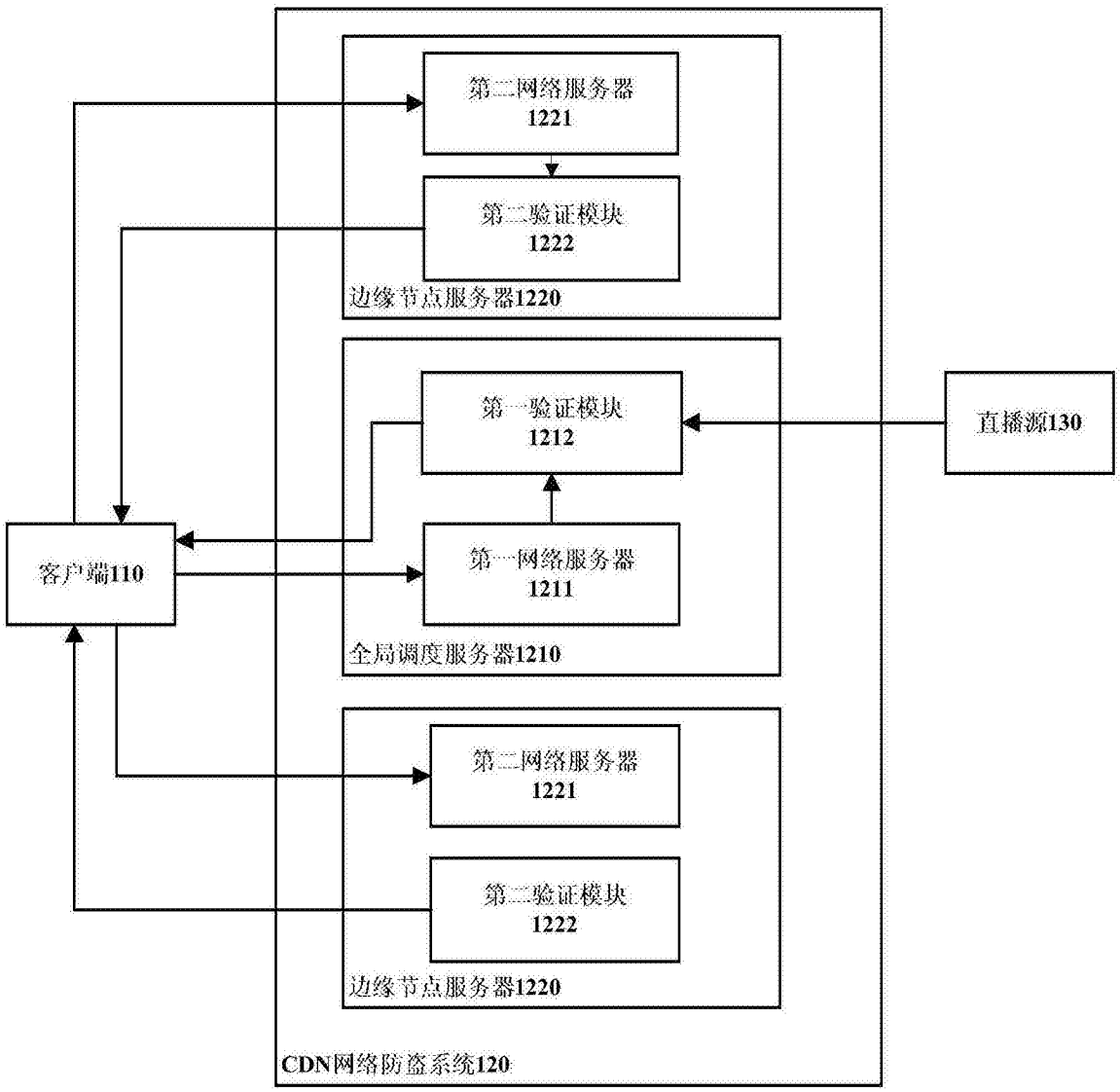

第二网络服务器
1221
第二验证模块
1222
边缘节点服务器1220
第一验证模块
1212
直播源130
客户端110
第一网络服务器
1211
全局调度服务器1210
第二网络服务器
1221
第二验证模块
1222
边缘节点服务器1220
CDN网络防盗系统120

图1

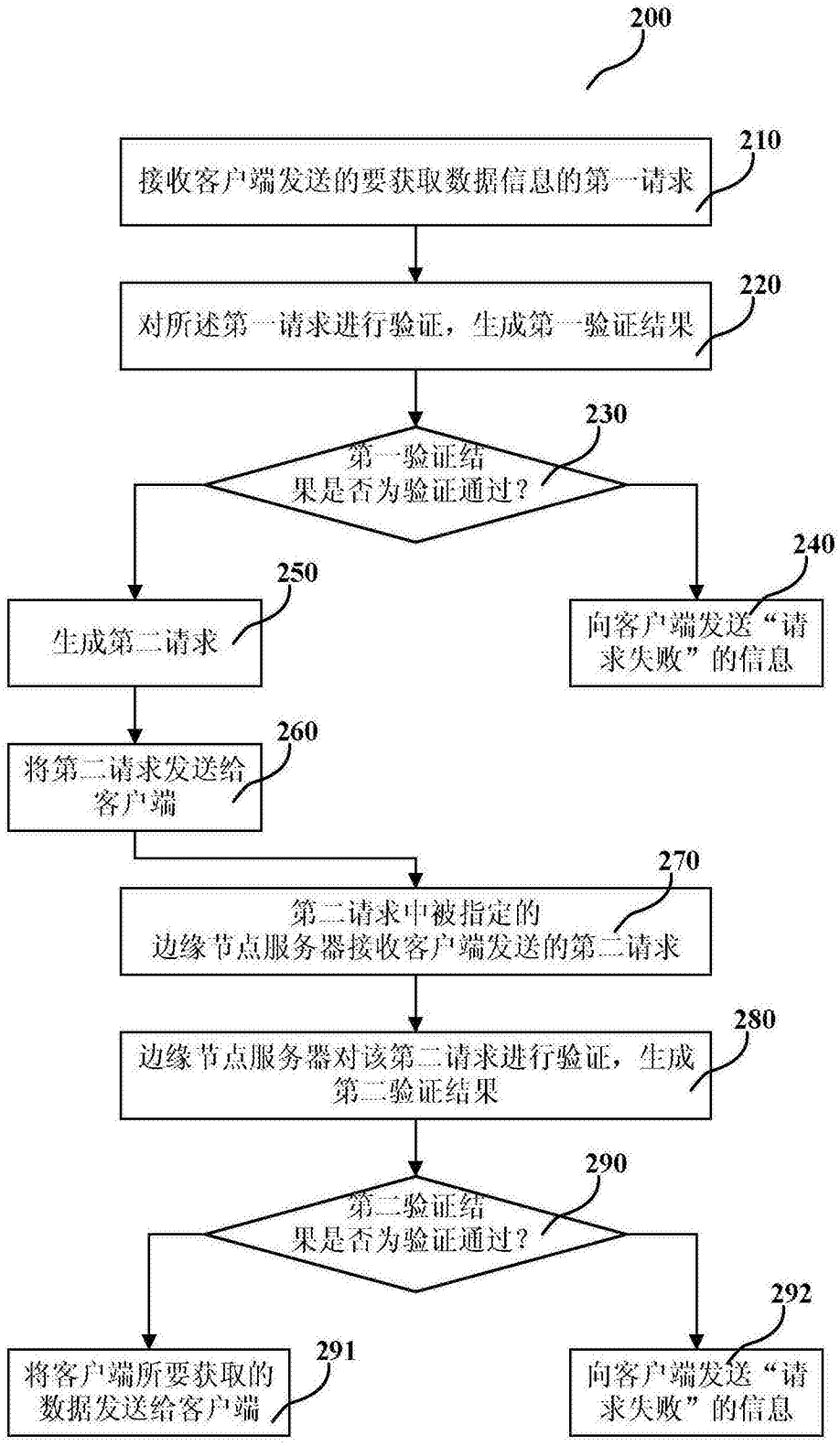

200
接收客户端发送的要获取数据信息的第一请求
210
对所述第一请求进行验证，生成第一验证结果
220
第一验证结果是否为验证通过？
230
向客户端发送“请求失败”的信息
240
生成第二请求
250
将第二请求发送给客户端
260
第二请求中被指定的边缘节点服务器接收客户端发送的第二请求
270
边缘节点服务器对该第二请求进行验证，生成第二验证结果
280
第二验证结果是否为验证通过？
290
将客户端所要获取的数据发送给客户端
291
向客户端发送“请求失败”的信息
292

图2