(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 104662871 A
(43)申请公布日 2015.05.27

(21)申请号 201380048527.5
(22)申请日 2013.09.16
(30)优先权数据
12306126.9 2012.09.18 EP
(85)PCT国际申请进入国家阶段日
2015.03.18
(86)PCT国际申请的申请数据
PCT/EP2013/069178 2013.09.16
(87)PCT国际申请的公布数据
WO2014/044641 EN 2014.03.27
(71)申请人 汤姆逊许可公司
地址 法国伊西莱穆利诺
(72)发明人 N. 勒斯库阿内克 E. 勒梅里尔 G. 斯特劳布
(74)专利代理机构 北京市柳沈律师事务所 11105
代理人 吕晓章
(51)Int.Cl.
H04L 29/08(2006.01)
H04L 29/06(2006.01)
H04W 28/08(2006.01)
H04W 36/22(2006.01)
H04W 88/06(2006.01)

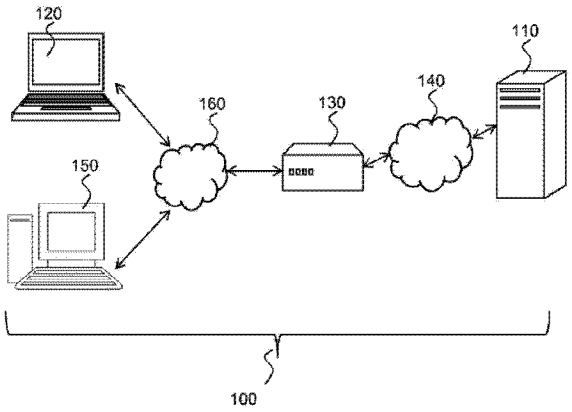
权利要求书2页 说明书6页 附图4页

(54)发明名称

安全地访问网络服务的方法和设备

(57)摘要

本发明涉及一种用于通过在用户设备上运行网络应用程序的浏览器通过网络来安全地访问网络服务的方法。所述网络服务至少是由其中本地设备正在被该用户设备访问的设备托管的。所述本地设备包含唯一地标识所述本地设备的全局名称和与该全局名称相关联的证书。该方法还包含通过对标识托管所述网络服务的任何设备的通用名称进行寻址来由网络应用程序向网络发送用于访问所述网络服务的请求的步骤；由网络应用程序从网络接收包含标识托管所述网络服务的所述本地设备的所述全局名称的对所述请求的响应的步骤；由网络应用程序检验所述接收的全局名称包含在名单中的步骤；以及当检验成功时，通过对所述全局名称进行寻址连接到所述本地设备的步骤；从所述本地设备接收所述证书的步骤；通过浏览器检验与所述全局名称相关联的所述证书的步骤和安全地访问所述网络服务的步骤。通用名称是一个根据其可访问任何本地设备的名称，即，对于托管网络服务的所有设备是通用的。所述名单包含被信任以用于托管网络服务的设备的全局名称。



CN 104662871 A

1. 一种用于通过在用户设备 (120) 上运行网络应用程序的浏览器通过网络 (160) 来安全地访问网络服务的方法，其中所述网络服务至少是由其中本地设备 (150,130) 正在被该用户设备访问的设备托管的，所述方法的特征在于，所述本地设备 (150,130) 包含唯一地标识所述本地设备的全局名称 (301) 和与该全局名称相关联的证书；该方法还包含：

通过对标识托管所述网络服务的任何设备的通用名称 (300) 进行寻址来由网络应用程序向网络 (160) 发送用于访问所述网络服务的请求；

由网络应用程序从网络 (160) 接收对所述请求的响应，所述响应包含标识托管所述网络服务的所述本地设备 (150,130) 的所述全局名称 (301)；

由网络应用程序检验所述接收的全局名称包含在名单中；

以及当检验成功时，通过对所述全局名称 (301) 进行寻址连接到所述本地设备 (150,130)；从所述本地设备接收所述证书；通过浏览器检验与所述全局名称相关联的所述证书和安全地访问所述网络服务。

2. 根据权利要求 1 所述的方法，其中，所述名单包含被信任以用于托管所述网络服务的设备的全局名称。

3. 根据权利要求 1 或 2 所述的方法，其中，由受信任的运营商向本地设备传送所述全局名称和与所述全局名称相关联的所述证书。

4. 根据权利要求 3 所述的方法，其中，通过在浏览器中运行的所述网络应用程序从所述受信任的运营商动态地获得所述名单。

5. 根据权利要求 3 所述的方法，其中，所述名单硬编码在在浏览器上运行的所述网络应用程序中。

6. 根据权利要求 1-5 中任一项所述的方法，其中，通过对所述全局名称 (301) 进行寻址连接到所述本地设备 (150,130) 还包含通过对全局名称 (301) 进行寻址来向外部网络 (140) 发送用于访问所述网络服务的第二请求；从该网络 (140) 接收对所述第二请求的响应，所述第二请求包含本地设备 (130,150) 的本地 IP 地址。

7. 根据权利要求 6 所述的方法，还包含在受信任运营商上公布与全局名称相关联的本地设备的本地 IP 地址的预备步骤。

8. 根据权利要求 6 或 7 所述的方法，其中通过由所述受信任运营商运行的 DNS 服务保留本地设备的本地 IP 地址和全局名称之间的映射。

9. 根据权利要求 1-8 中任一项所述的方法，其中，所述用于通过对通用名称进行寻址来访问所述网络服务的所述请求是 HTTP 请求。

10. 根据权利要求 1-9 中任一项所述的方法，其中，用于通过对所述全局名称进行寻址来安全地访问网络服务的请求是 HTTPS 请求。

11. 根据权利要求 1-10 中任一项所述的方法，其中，所述本地设备是网关。

12. 一种用于通过运行网络应用程序的浏览器通过网络来安全地访问网络服务的用户设备 (120,400)，所述网络服务至少是由其中本地设备正在被该用户设备访问的设备托管的，所述设备包含：

通过对标识托管所述网络服务的任何设备的通用名称进行寻址来由网络应用程序向网络发送用于访问所述网络服务的请求的部件；

由网络应用程序从网络接收包含对托管所述网络服务的所述本地设备进行唯一标识

的全局名称的对所述请求的响应的部件；

由网络应用程序检验所述接收的全局名称包含在名单中的部件，其中所述名单包含被信任以用于托管所述网络服务的设备的全局名称；通过对所述全局名称进行寻址通过网络应用程序连接到所述本地设备的部件；用于接收从所述本地设备接收的证书的部件以及用于通过浏览器检验与所述全局名称相关联的所述证书的部件以及用于安全地访问所述网络服务的部件。

安全地访问网络服务的方法和设备

技术领域

[0001] 本发明一般地涉及对网络 (web) 服务的安全访问的领域。更确切地说，本发明涉及一种用于通过在用户设备上运行网络应用程序的浏览器通过网络来安全地访问网络服务的方法，其中，所述网络服务是由本地设备托管的。

背景技术

[0002] 本节旨在向读者介绍本领域的各个方面，其可以与下面所描述和 / 或要求保护的本发明的各个方面有关。本讨论被认为是有助于向读者提供背景信息以便于更好地理解本发明的各个方面。因此，应当理解，这些陈述要从这个角度阅读，而不是作为对现有技术的承认。

[0003] 数字数据（例如，图片，视频等）越来越多地在移动设备（例如，智能手机，平板电脑，膝上型计算机）上产生和进行管理。这些数据也经常经由因特网被共享、备份或处理。事实上，许多“云”服务处理用户的内容，无论是图片处理服务、社交网络或在线存储。这些云服务的大多数完全依靠网络技术。其结果是，用户需要通过 HTTP 上传大量内容到网络应用程序。然而，上传的速度是被可用带宽所限制的。实际上，由于对传统基础设施 (xDSL) 或对共享介质（网状）的使用，导致到因特网的连接速度仍然是有限的。

[0004] 长上传时间使得用户不能让其独立的设备待机或断电，并要求这些用户使其设备保持连接以处理通过因特网的传输转。为了缓解这些问题，提出了一种将通过 HTTP 的上传卸载到永久连接到网络的第三方设备（例如住宅网关）的机制。因此，提出了一种用于定位提供对网络服务的卸载的第三方设备的方法。

[0005] 然而，将任务卸载到第三方需要信任此第三方，换句话说，托管卸载服务的第三方设备必须由用户的独立的设备进行验证。用于对设备或网络服务进行验证的已知解决方案是基于信任权威机构的认证。证书由信任权威机构传送给拥有网络服务的受信任的运营商或传送给用户的物理设备。然而，这些解决方案与诸如网络浏览器的传统软件，以及其中处理环境有限的标准的网络协议不兼容。换句话说，浏览器在输入和输出方面受到限制，例如，浏览器不能访问该浏览器在其上执行的设备的存储介质（诸如硬盘驱动器），不能直接访问网络。

[0006] 因此需要一种用于通过在用户设备上运行网络应用程序的浏览器通过网络来安全地访问网络服务，其中，所述网络服务是由本地设备托管的解决方案。该方法应该刻意简单以便于实施和使用，并与传统软件兼容，适于以 JavaScript 实现，并在浏览器中运行。

[0007] 本发明提供了这样的解决方案。

发明内容

[0008] 在第一方面，本发明涉及一种用于通过在用户设备上运行网络应用程序的浏览器通过网络来安全地访问网络服务的方法。所述网络服务至少是由其中本地设备正在被该用户设备访问的设备托管的。有利地，该本地设备是托管网络服务和最接近该用户设备的设

备。本地设备包含唯一地标识所述本地设备的全局名称和与该全局名称相关联的证书。该方法还包含通过对标识托管网络服务的任何设备的通用名称进行寻址来由网络应用程序向网络发送用于访问网络服务的请求的步骤；由网络应用程序从网络接收包含标识托管网络服务的本地设备的所述全局名称的对请求的响应的步骤；由网络应用程序检验所接收的全局名称包含在名单中的步骤；以及，当检验成功时，通过对全局名称进行寻址连接到本地设备的步骤；从本地设备接收证书的步骤；通过浏览器检验与全局名称相关联的证书的步骤和安全地访问网络服务的步骤。有利地，通用名称是根据其可访问任何本地设备的名称，即，对于托管网络服务的所有设备是通用的。有利地，所述名单，也被称为白名单，包含被信任以用于托管网络服务的设备的全局名称。有利地，该名单不包含被信任以用于托管网络服务的本地设备的全局名称的详尽名单，因为全局名称的数量可能是巨大的，但用于匹配本地设备的全局名称的模式 (pattern)。

[0009] 根据有利的特征，由受信任的运营商向本地设备传送全局名称和与全局名称相关联的证书。

[0010] 根据另一有利的特征，通过在浏览器中运行的网络应用程序从受信任的运营商动态地获得该白名单。在一个变型中，所述白名单硬编码在在浏览器上运行的网络应用程序中。

[0011] 在第一优选实施例中，用于通过对通用名称进行寻址来访问该网络服务的请求是 HTTP 请求，并且用于通过对全局名称进行寻址来安全地访问所述网络服务的请求是包括 SSL 请求的 HTTPS 请求。

[0012] 根据变型，本地设备是网关设备、机顶盒、网络附接存储器 (NAS)。

[0013] 在第二方面，本发明涉及一种用于通过运行网络应用程序的浏览器通过网络来安全地访问网络服务的用户设备。所述网络服务至少是由其中本地设备正在被该用户设备访问的设备托管的。有利地，该本地设备是托管网络服务和最接近该用户设备的设备。该设备包含通过对标识托管网络服务的任何设备的通用名称进行寻址来由网络应用程序向网络发送用于访问网络服务的请求的部件；由网络应用程序从网络接收包含对托管网络服务的本地设备进行唯一标识的全局名称的对请求的响应的部件；由网络应用程序检验所接收的全局名称包含在名单（也被称为白名单）中的部件，其中该名单包含被信任以用于托管网络服务的本地设备的全局名称；以及通过对全局名称进行寻址通过网络应用程序连接到本地设备的部件；从本地设备接收证书的部件和检验与全局名称相关联的证书的部件以及用于安全地访问网络服务的部件。

[0014] 对于用于通过在用户设备上运行网络应用程序的浏览器通过网络来安全地访问网络服务的方法所描述的任何特征或实施例与适于实施所公开方法的用户设备或本地设备是兼容的，其中所述网络服务是由本地设备托管的。

[0015] 有利地，根据第一实施例的方法是与当前软件和标准网络协议兼容的。因此，它可以被部署，而无需改变该用户的浏览器或者所使用的协议。

附图说明

[0016] 现在将通过非限制性示例的方式，参考附图，描述本发明的优选特征，附图中：

[0017] 图 1 示出了可以使用本发明的示例性网络；

[0018] 图 2 示出了根据本发明第一实施例的安全访问方法的步骤；

[0019] 图 3 示出了根据本发明优选实施例的安全访问方法的步骤；以及

[0020] 图 4 示出了根据本发明优选实施例的实现安全访问方法的本地设备。

具体实施方式

[0021] 图 1 示出可以使用本发明的示例性网络 100。网络 100 包含托管诸如图片共享应用程序的网络应用程序的服务器设备 110。用户拥有在其上有可用网络浏览器的诸如电池供电的设备（平板电脑、膝上型计算机、移动电话）或计算机的个人设备 120。例如图片共享应用程序的网络应用程序的客户端部分在用户设备 120 的浏览器上执行并且该网络应用程序访问该网络应用程序的该服务器部分。该网络应用程序的该客户端部分还可以访问网络服务，诸如卸载服务。用户设备通过局域网 160 连接到运行在诸如因特网路由器、机顶盒、其他用户计算机、住宅网关、NAS 150 的本地设备上的网络服务。该网络应用程序的该客户端部分和网络服务可以通过诸如无线因特网路由器或住宅网关的网络接入设备 130 访问该网络应用程序的该服务器部分。因此，住宅网关是在快速局域网 160 和相对慢的宽带网络 140 之间的前沿 (frontier)，其中到该慢的宽带网络的接入对于上传数据到网络应用程序的服务器部分是一个问题。在优选实施例中，网络接入设备 130 是本地设备，因为网络接入设备总是通电的。例如，在其中这样的网络接入设备 130 不支持卸载功能的变型中，本地设备是任何类型的本地网络 140 的设备，优选地是如上详述的总是开启的类型，例如 NAS 150。本发明提供了一种解决方案，用于验证本地设备 130、150 或更确切地说运行在本地设备 130、150 上的网络服务，以使得通过避免攻击者冒充本地设备而保护在本地设备中临时经过的上传的数据免受攻击。

[0022] 本发明的一个显著的发明构思是从浏览器定位要在网络应用程序内使用的本地网络服务，并对该本地服务进行验证。该方法可以用于定位卸载服务，但它有利地是与诸如定位网络到 DLNA/UPNP 中继的其他应用程序是兼容的，其中网络应用程序被授权通过到 DLNA/UPNP 中继的网络服务来控制用户设备。

[0023] 在优选的实施例中，该方法适于由 JavaScript 语言来执行。因此该方法有利地适于安装到由网络浏览器所提供的受约束的执行环境中。这些约束有助于浏览器确保任何恶意代码具有非常有限的权力。

[0024] 此外，用于安全地访问网络服务的该方法动态地确定服务的存在和它的地址两者。该机制还负责验证重新定位的服务。该机构还允许根据服务的存在实现网络应用程序的客户端部分的动态适应。

[0025] 图 2 示出了根据本发明第一实施例的安全访问方法的步骤。

[0026] 浏览器只能使用实施在所谓的浏览器网络 API 中的 XMLHttpReq 访问网络。浏览器还包括 JavaScript 机器。存在于浏览器中的验证 / 认证机制是 TLS/SSL 机制。

[0027] 在未在图 2 表示的预备步骤中，受信任运营商购买了域名 (offload.org)，并请求该域名的 SSL 证书。运行该服务的每个受信任设备接收唯一的名称（例如 af34a），以及对应于其名称的证书 (af34a.offload.org)。受信任运营商运行受信任设备能够更新的 DNS 服务（在因特网上可用），以便该名称 af34a.offload.org 始终映射到正确的本地 IP 地址。

[0028] 在该位置 / 验证过程的第一步骤 210 中，试图访问本地托管的网络服务的浏览器

发送对通用名称 (offload.local) 的请求到网络。更确切地，JavaScript 通过浏览器网络 API 发出本地查询到对在任何本地网络上运行服务的任何设备通用的一些固定的地址 (offload.local)。存在于网关中的 DNS 将用本地 IP 地址回复该 DNS 查询，并且浏览器网络 API 连接到该 IP 地址，即，使用不安全的 HTTP 协议连接到托管网络服务的本地设备的 IP 地址。问题在于，不可能得到“offload.local”的证书，因为这个名称不属于任何人，也没有认证权威机构将传送这种证书。

[0029] 因此，在第二步骤 220 中，浏览器获得由本地设备托管和与本地设备 IP 地址关联的网络服务的完全合格的名称 (af34a.offload.org)，称为全局名称。然而，正如已经解释过的，完全合格的名称可能会被破坏。

[0030] 在第三步骤 230 中，浏览器检查所获得的全局名称 (af34a.offload.org) 是由某些受信任运营商管理。事实上，虽然有人可能有 hacker.org 的有效证书，但这不是充分条件。进一步的要求是，该证书的所有者是可信的。因此，浏览器将针对白名单来检验所获得的全局名称，以保证子证书 (af34a.offload.org) 来自受信任运营商 (offload.org)。本领域技术人员将认识到，白名单可以不包含每个受信任设备的全局名称的详尽名单，而是包含用来检验全局名称的方案匹配模式。

[0031] 在最后的步骤 240 中，当检验成功时，浏览器发送对于安全地访问该全局名称的请求。更确切地说，浏览器网络 API 执行对完全合格的名称 (af34a.offload.org) 的新的查询。由受信任运营商操作的 DNS 以本地 IP 地址应答。浏览器以 HTTPS 连接到此本地 IP 地址，并使用该浏览器的证书集合检查与该全局名称相关联的证书对应于它所连接的设备和该证书是有效的并且未被撤销。有利地，步骤 240 允许验证本地设备，并且有利地，步骤 230 允许受信任运营商批准本地设备。

[0032] 因此，保险和安全地使用在 https://af34a.offload.org 可用的网络服务。

[0033] 任何步骤的任何失败意味着该服务是不可用的或它由于一些验证问题而不能被信任。因此，不应使用它。

[0034] 图 3 示出根据本发明的优选实施例的安全访问的步骤。如已经说明的，在优选实施例中，网络服务是用于卸载上传的网络服务。

[0035] 位置服务在固定的URL http://offload.local/test 可用。为清楚起见，我们省略在整个描述中的端口号。然而，为了避免与现有的服务发生冲突，使用非标准的HTTP/HTTPS 端口（例如，对于 HTTP 是 8787 和对于 HTTPS 是 8788）。完全合格的名称和端口是固定的，并且对于所有网关是通用的。因此，在只能使用 XMLHttpRequest 访问网络的浏览器中运行的网络应用程序可以访问该服务。浏览器将该通用的完全合格的名称 (offload.local 300) 解析为网关的 IP 地址，并连接它。任何连接错误（失败的 DNS 解析、连接超时、404，403……）表明该服务不可用。如果卸载服务正在运行，并能接受卸载请求，浏览器会收到“可以”作为应答。

[0036] 位置服务在很大程度上依赖于 DNS 将固定名称解析为支持局域网上的服务的设备的 IP 地址。大多数网关运行它们自己的 DNS 服务器，因此可以自己注册为 offload.local。如果卸载服务是由另一设备提供的，由于 DHCP 协议，该设备仍会将名称 offload.local 注册在网关的 DNS 中。由于 DNS 解析会容易地受在同一个局域网上使用 DHCP 为 offload.local 注册的任何人影响，网络开发人员可能愿意确保该解析产生受信任（根据

浏览器的 SSL 证书）网关。解决方案是依靠 HTTPS 验证机制。为此，每个网关都有它自己的自签名的证书，并且用户从其信任的网关手动添加证书到他的浏览器证书名单。请求被发送到 https://offload.local/ 而不是 http://offload.local/。如果网关不被信任，对位置服务的请求将导致连接错误。因此，卸载将无法启用。然而，该处理要求用户通过在他的浏览器中添加适当的证书来手动批准他使用的每个新网关。这个处理可能是棘手的，并阻止完全透明的用户体验。

[0037] 为了使这一处理是无缝的，根据优选实施例的方法有利地提供了一种增强的位置方法，该方法也需要验证网关。该方法旨在与运行受信任软件并且其证书不能被复制的嵌入式设备一起使用。图 3 示出了整个位置和验证处理。这个处理增强了在此之前描述的非验证位置服务。在这种情况下，每个网关与唯一的名称（例如 af34a.offload.org 301）相关联，并且具有由受信任验证权威机构签名的对应证书。每个网关将其本地 IP 地址发布到运行用于受信任域名 offload.org 的动态 DNS 服务。

[0038] 这个处理现在在于定位网关以及然后验证它。为此，发出到 http://offload.local/auth 的请求。该请求返回网关的唯一的完全合格名称（例如，af34a.offload.org 301）。该完全合格的名称与域名的白名单进行匹配，以确保证书是由适当的验证权威机构所发出：不是所有的有效 SSL 域名（即，根据浏览器证书名单所批准的）映射到受信任网关。只有少数域名（例如，offload.org）是出于此目的而受信任的，并且因此被列在白名单中。至此，网关不被信任并且所获得的信息可能已被操纵。然而，完全合格的名称映射到受信任的一组网关。接着，发出到 https://af34a.offload.org/test 的请求。浏览器检查网关的证书，从而防止任何劫持。如果证书是合法的，可以启用卸载机制并且所述要求可以被发布到 https://af34a.offload.org/upload/。

[0039] 再次地，如同在基本位置处理中，任何错误意味着卸载机制不能被启用。因为每个设备有其自己的证书，因此可以在个体证书被窃取的情况下，或者在设备子集中发现安全问题的情况下，撤销该个体证书。至多地，如果攻击者通过篡改 DNS 项成功地中断位置服务，网络应用程序将简单地回落到不具有卸载能力的正常服务，从而导致除了卸载不起作用外，对用户来说没有服务中断。

[0040] 本领域技术人员也将理解，因为该方法可以很容易地实现而无需特殊装置，因此它可以通过诸如个人计算机、移动电话、家庭网络网关等的“正常”的用户设备实现。本发明进一步与 802.11 通信 (Wi-Fi)、或诸如蓝牙或 UWB 的任何有线或无线接入兼容。有利地，本发明与位于无线网络热点上的网络服务兼容。

[0041] 图 4 示出了根据本发明优选实施例的示例性用户设备。用户设备 400 包含被称为浏览器或网络浏览器的软件模块。浏览器运行试图通过网络安全地访问网络服务的网络应用程序。根据不同的变型，用户设备可以实现在计算机、移动设备、平板电脑上。

[0042] 用户设备 400 包含诸如 802.11 无线网卡的网络接口 410、至少一个处理器 420（下文中称为“处理器”）和存储器 430。网络接口 410 适于将用户设备连接到网络，从而将用户设备连接至本地设备。例如，网络接口 410 物理地发送用于访问远程网络服务的请求和物理地接收对该请求的响应。在变型中，网络接口 410 是诸如以太网的有线接口。处理器 420 适于执行实施被称为网络浏览器的软件模块的指令。网络浏览器适于运行网络应用程序。在下文只对理解本发明的所必须的特征进行详细描述。网络应用程序通过网络接口 410 发

送请求以通过对标识托管网络服务的任何设备的通用名称进行寻址来访问网络服务。网络应用程序通过网络接口 410 接收包含唯一地标识托管网络服务的本地设备和该用户设备可以安全地访问的全局名称的对该请求的响应。网络应用程序检验所接收的全局名称包含在包括受信任用于托管该网络服务的设备的全局名称的名单中。有利地，该名单存储在存储器 430 中。网络应用程序通过对全局名称进行寻址建立通过网络接口 410 到本地设备的连接，并且浏览器检验所接收的与本地设备的全局名称相关联的证书。因此，网络应用程序安全地访问网络服务。在变型中，所述安全功能实现在诸如安全处理器的硬件中。

[0043] 所述描述集中在上传到网络应用程序，但是，本发明与其中网络服务是本地提供的机制也是兼容的。

[0044] 在说明书和（在适当情况下）权利要求书以及附图中公开的每个特征可以独立地或以任何适当的组合来提供。描述为以软件实现的特征也可以在硬件中实现，反之亦然。权利要求书中出现的附图标记仅仅是说明的方式，并应当对权利要求的范围没有限制作用。

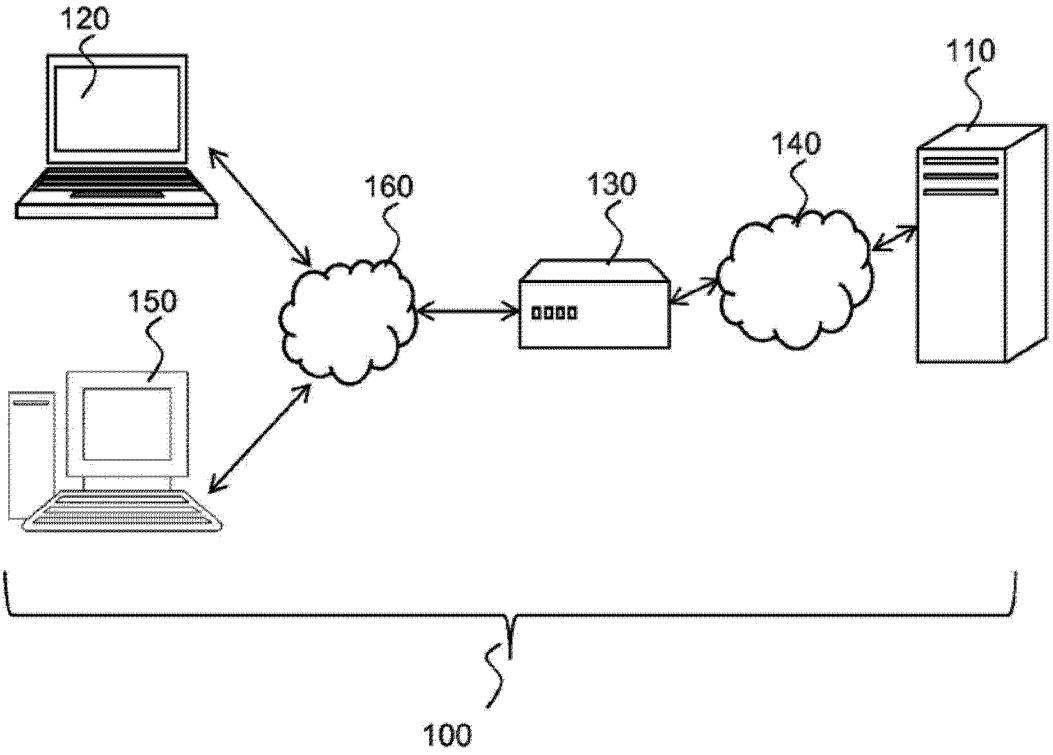


图 1

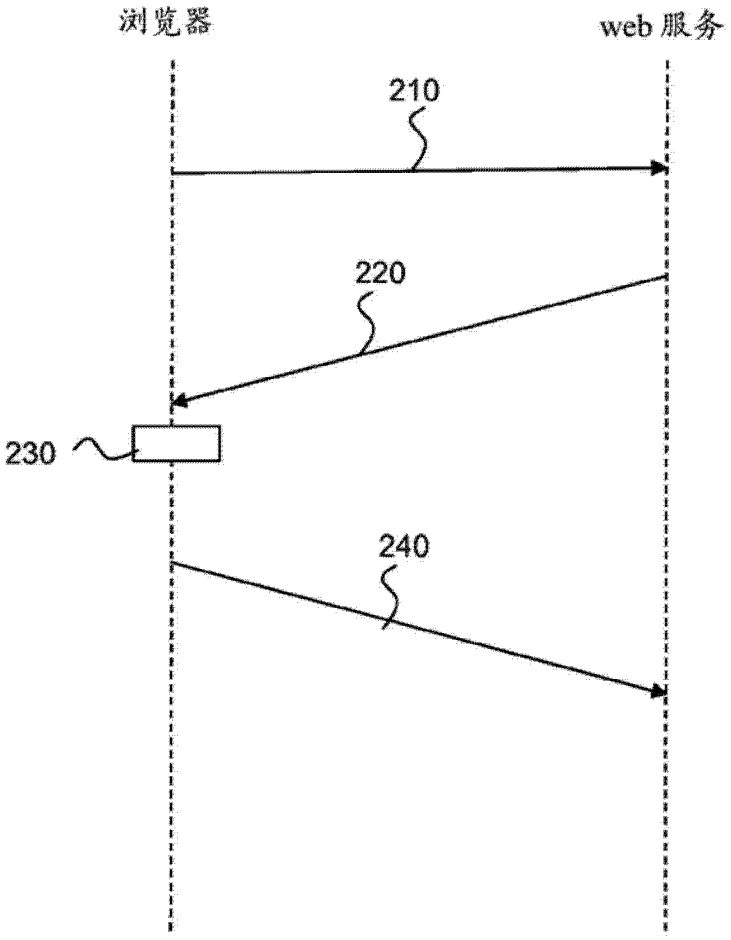


图 2

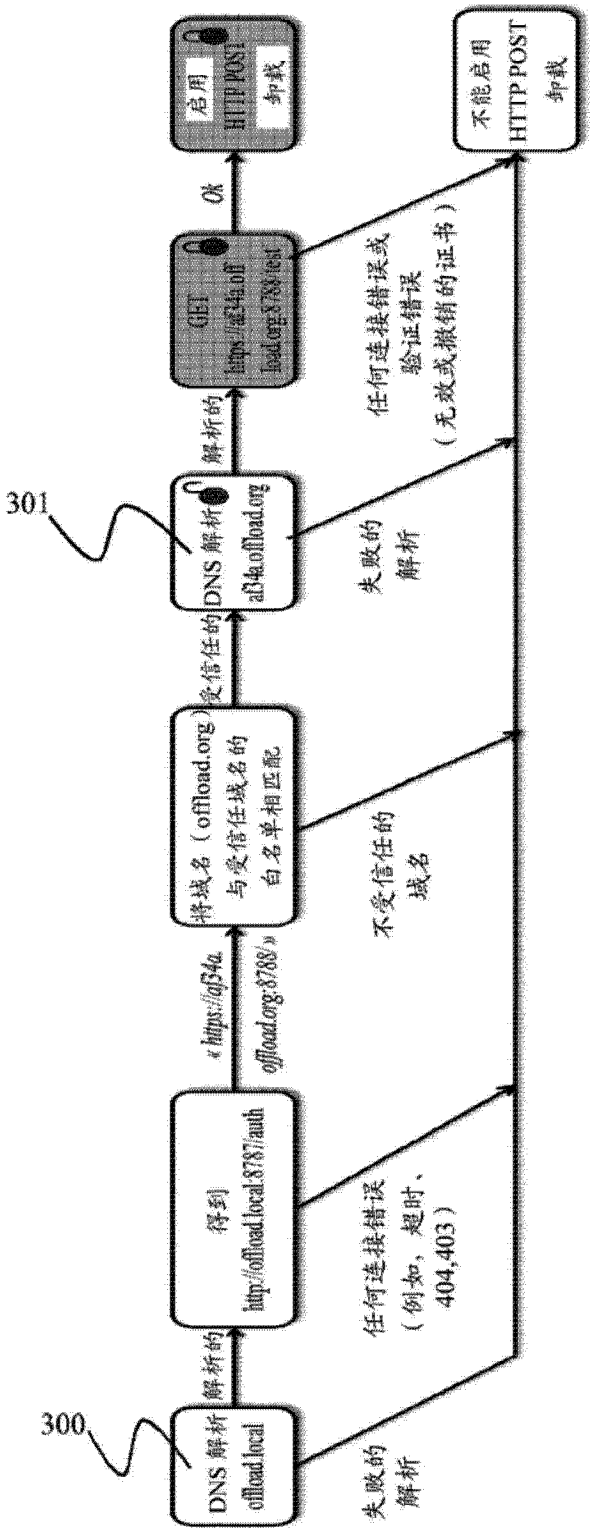

300
DNS 解析
offload.local
失败的
解析
解析的
得到
http://offload.local:8787/auth
任何连接错误
（例如，超时、
404,403）
« https://ql34.
offload.org:8788/ »
持域名（offload.org）
与受信任域名的
白名单相匹配
不受信任的
域名
受信任的
301
DNS 解析
ql34.offload.org
失败的
解析
解析的
GET
https://ql34.off
load.org:8788/test
任何连接错误或
验证错误
（无效或撤销的证书）
OK
启用
HTTP POST
卸载
不能启用
HTTP POST
卸载

图 3

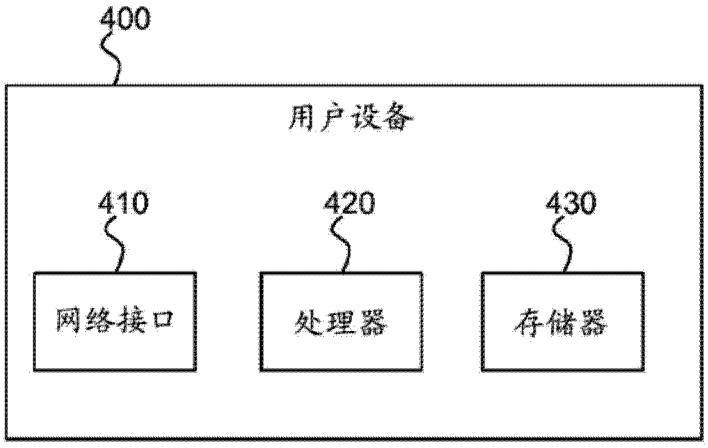


图 4