(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 104584011 B
(45)授权公告日 2018.09.18

(21)申请号 201380044936.8

(22)申请日 2013.06.27

(65)同一申请的已公布的文献号
申请公布号 CN 104584011 A

(43)申请公布日 2015.04.29

(30)优先权数据
13/536285 2012.06.28 US

(85)PCT国际申请进入国家阶段日
2015.02.27

(86)PCT国际申请的申请数据
PCT/US2013/048366 2013.06.27

(87)PCT国际申请的公布数据
WO2014/004926 EN 2014.01.03

(73)专利权人 茨特里克斯系统公司
地址 美国佛罗里达州

(72)发明人 G.措利斯

(74)专利代理机构 中国专利代理(香港)有限公司 72001
代理人 臧永杰 陈岚

(51)Int.Cl.
G06F 17/30(2006.01)

(56)对比文件
CN 101472223 A,2009.07.01,
WO 2008075883 A1,2008.06.26,
CN 1892653 A,2007.01.10,

审查员 何华

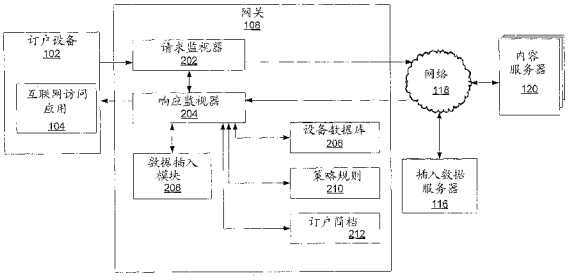
权利要求书2页 说明书9页 附图9页

(54)发明名称

用于WEB内容和WEB服务的安全网络内插入的方法和系统

(57)摘要

提供一种web内容和web服务插入的方法。所述方法包括:接收响应于请求数据而发送的响应数据,其中响应数据包括响应报头和第一网页。所述方法还包括:在确定了插入数据要与第一网页一起被包括之后,通过将插入数据添加到第一网页而更新响应数据。插入数据包括标识脚本的脚本元素,所述脚本包括在第一网页内显示第二网页的指令。所述方法还包括提供更新的响应数据。



CN 104584011 B

1.一种web内容和web服务插入的方法,所述方法包括:

接收响应于请求数据而发送的响应数据,其中响应数据包括响应报头和第一网页;

在确定要将插入数据包括在第一网页中之后,通过将插入数据添加到第一网页中来更新响应数据,所述插入数据包括标识脚本的脚本元素,所述脚本包括在第一网页内显示第二网页的指令,其中所述脚本进一步包括将与第二网页相关联的内联框架添加到第一网页的指令,以及其中在具有第一互联网地址的指定服务器上托管脚本和第二网页;

修改所述响应数据以指示允许从所述指定服务器上托管的所述第二网页发出的一个或多个请求;以及

提供更新的响应数据。

2.根据权利要求1所述的方法,其中所述脚本元素通过指定第一互联网地址标识所述脚本,并且用于显示第二网页的指令包括第一互联网地址。

3.根据权利要求1所述的方法,还包括接收请求数据,其中请求数据包括请求报头。

4.根据权利要求3所述的方法,其中确定要将插入数据包括在第一网页中至少基于请求报头。

5.根据权利要求3所述的方法,其中标识脚本包括指定第二互联网地址,并且用于显示第二网页的指令包括第二互联网地址,所述方法还包括:

通过用第一互联网地址替换请求数据内第二互联网地址的任何出现而更新请求数据;以及

提供更新的请求数据。

6.根据权利要求3所述的方法,其中第二网页包括一个或多个web服务调用,所述方法还包括:

将使能web服务调用的指令添加到响应报头。

7.一种存储指令的非暂时性计算机可读介质,所述指令在由计算机执行时使得计算机执行web内容和web服务插入的方法,所述方法包括:

接收响应于请求数据而发送的响应数据,其中响应数据包括响应报头和第一网页;

在确定要将插入数据包括在第一网页中之后,通过将插入数据添加到第一网页来更新响应数据,插入数据包括标识脚本的脚本元素,所述脚本包括在第一网页内显示第二网页的指令;

其中所述脚本进一步包括将与第二网页相关联的内联框架添加到第一网页的指令,以及其中在具有第一互联网地址的指定服务器上托管脚本和第二网页;

修改所述响应数据以指示允许从所述指定服务器上托管的所述第二网页发出的一个或多个请求;以及

提供更新的响应数据。

8.根据权利要求7所述的非暂时性计算机可读介质,其中所述脚本元素通过指定第一互联网地址标识所述脚本,并且显示第二网页的指令包括第一互联网地址。

9.根据权利要求7所述的非暂时性计算机可读介质,还包括接收请求数据,其中请求数据包括请求报头。

10.根据权利要求9所述的非暂时性计算机可读介质,其中插确定要将插入数据包括在第一网页中至少基于所述请求报头。

11.根据权利要求9所述的非暂时性计算机可读介质，其中标识脚本包括指定第二互联网地址，并且显示第二网页的指令包括第二互联网地址，所述方法还包括：

通过用第一互联网地址替换请求数据内第二互联网地址的任何出现而更新请求数据；以及

提供更新的请求数据。

12.根据权利要求9所述的非暂时性计算机可读介质，其中第二网页包括一个或多个web服务调用，所述方法还包括：

将使能web服务调用的指令添加到响应报头。

13.一种耦合到第一网络和第二网络的网关，所述网关包括响应监视器，所述响应监视器被配置成：

从第二网络接收响应于请求数据而发送的响应数据，其中响应数据包括响应报头和第一网页；

在确定要将插入数据包括在第一网页中之后，通过将插入数据添加到第一网页中来更新响应数据，所述插入数据包括标识脚本的脚本元素，所述脚本包括在第一网页内显示第二网页的指令，其中所述脚本进一步包括将与第二网页相关联的内联框架添加到第一网页的指令，以及其中在具有第一互联网地址的指定服务器上托管脚本和第二网页；

修改所述响应数据以指示允许从所述指定服务器上托管的所述第二网页发出的一个或多个请求；以及

向第一网络提供更新的响应数据。

14.根据权利要求13所述的网关，其中标识脚本包括指定第一互联网地址，并且用于显示第二网页的指令包括第一互联网地址。

15.根据权利要求13所述的网关，还包括：被配置成从第一网络接收请求数据的请求监视器，其中所述请求数据包括请求报头。

16.根据权利要求15所述的网关，其中确定要将插入数据包括在第一网页中至少基于请求报头。

17.根据权利要求15所述的网关，其中标识脚本包括指定第二互联网地址，并且用于显示第二网页的指令包括第二互联网地址，并且其中请求监视器还被配置成：

通过用第一互联网地址替换请求数据内第二互联网地址的任何出现而更新请求数据；以及

向第二网络提供更新的请求数据。

18.根据权利要求15所述的网关，其中第二网页包括一个或多个web服务调用，并且其中响应监视器还被配置成：将使能web服务调用的指令添加到响应报头。

用于WEB内容和WEB服务的安全网络内插入的方法和系统

背景技术

[0001] 万维网(“Web”)已经从通过超链接互连的静态文档的集合演变到使能在用户和内容提供商之间的无缝信息共享和协同的环境,其中域、web站点、应用和服务之间的界限是模糊的。许多应用正迁移到服务器基础设施(“云(Cloud)”),并且不再需要软件的本地安装或本地存储。尽管允许终端用户获得对Web应用和服务的访问的移动应用(“App”)的激增,Web浏览器(“浏览器(Browser)”)仍然是用于获得Web内容的目的的主要应用。

[0002] 如今,由人们在其日常生活中采用的诸如台式、膝上式和上网本电脑、智能电话和功能电话、触摸屏平板设备和电子书阅读器、游戏控制台、高端车和电视之类的大多数电子设备配备有浏览器,其充当对互联网的进入点,不仅以有线方式,而且日益更多以无线方式如此。

[0003] 互联网服务提供商(“ISP”)和移动网络运营商(“MNO”)一直在寻找区分他们自己并增强其订户的体验的方式。例如,ISP和MNO想要向他们的订户递送集成的云应用和服务、定制的消息和通知、广告和促销内容等等。

附图说明

[0004] 图1图示示范性系统的框图。

[0005] 图2是图示在图1的示范性系统中的示范性安全网络内web内容插入方案的实施例的框图。

[0006] 图3A图示示范性的原始网页的实施例。

[0007] 图3B图示示范性的修改的网页的实施例。

[0008] 图4图示示范性的JavaScript脚本的实施例。

[0009] 图5A、5B、5C和5D图示修改的网页内的插入的web内容的示范性可视配置的不同实施例。

[0010] 图6图示示范性插入数据服务器及在其上托管的文件的实施例。

[0011] 图7是表示web内容和web服务的安全网络内插入的示范性方法的流程图。

具体实施方式

[0012] 现在将对示范性实施例详细地做出参考,在附图中图示其示例。只要可能,将遍及附图使用相同的参考标号来指代相同或相像的部分。

[0013] 本文公开的示范性实施例目的在于用于web内容和web服务到由订户请求的原始网页中的安全网络内插入的方法和系统。插入方法对请求的网页的所有者是透明的,并且它对订户也是无缝的,因为它不需要安装附加软件或浏览器插件(外接附件(add-on))。插入方法可以顺从行业标准,诸如由互联网工程任务组(“IETF”)和万维网联盟(“W3C”)公布的行业标准。此外,插入方法保留原始网页和插入的web内容二者的安全性和完整性。

[0014] 图1是示范性的系统的框图。除了其它事物以外,示范性的系统可以包括订户设备102、网关108、一个或多个内容服务器120、网络106和118以及互联网访问应用104。网关108

可以耦合到网络106和网络118二者，网络118可以另外耦合到内容服务器120和插入数据服务器116，并且网络106可以另外耦合到订户设备102。订户设备102可以包括或耦合到互联网访问应用104。

[0015] 订户设备102是具有联网能力的计算机程序或硬件设备。例如，订户设备102可以是台式、膝上式或上网本电脑、智能电话、功能电话、触摸屏平板设备、电子书阅读器、游戏控制台、高端车、电视等等。订户设备102可以从互联网访问应用104接收请求数据，将该数据传输到远程设备，响应于请求数据而接收响应数据，并将响应数据提供回到互联网访问应用104。可以通过诸如HTTP之类的任何合适的通信协议来传输请求数据和响应数据。订户设备102还可以包括显示器，所述显示器可以由互联网访问应用用来向订户(用户)呈现接收的响应数据。

[0016] 互联网访问应用104是客户端应用，诸如浏览器、移动app或可以访问远程web内容并将该内容呈现给订户的任何其它软件和/或硬件应用。互联网访问应用104可以运行在订户设备102上或者在云上，也就是说，在例如通过网络106耦合到订户设备102的远程设备(未示出)上。互联网访问应用104可以从订户接收命令，向订户设备102传递对应于命令的请求数据，响应于请求数据而从订户设备102接收响应数据，并向订户呈现响应数据。

[0017] 请求数据可以包括统一资源标识符(“URI”)，其标识特定资源(例如网页、脚本或服务)和托管特定资源的远程服务器。除了其它事物以外，响应数据可以包括请求的特定资源。

[0018] 网络106和118可以是任何类型的网络，包括但不限于适合于诸如互联网通信之类的联网通信的广域网(WAN)、局域网(LAN)或无线网络的任何组合。

[0019] 网关108是可以拦截、分析和操纵在网络106和118之间交换的数据的一个或多个网络设备。网关108可以由ISP/MNO用来递送关于拦截的数据的各种服务，诸如web内容插入、应用检测、带宽节制、入侵/恶意软件检测、防火墙、网络地址转化和业务优化。此外，网关108可以充当用于“控制平面”接口的集成点，诸如认证、授权和计费(“AAA”)。网关108还能够可以访问ISP/MNO订户简档储存库(“SPR”)，要么经由策略和收费规则框架(PCRF)基础设施，要么直接使用各种数据库或目录(例如LDAP)访问协议。

[0020] 网关108可以具有一个或多个处理器和用于存储程序指令的至少一个存储器。(一个或多个)处理器可以是单个或多个微处理器、现场可编程门阵列(FPGA)或能够执行特定指令集的数字信号处理器(DSP)。计算机可读指令可以存储在有形的非暂时性计算机可读介质上，诸如软盘、硬盘、CD-ROM(致密盘-只读存储器)以及MO(磁-光)、DVD-ROM(数字通用盘-只读存储器)、DVD-RAM(数字通用盘-随机存取存储器)或半导体存储器。替代地，方法可以在硬件组件中或诸如例如ASIC、专用计算机或通用计算机之类的硬件和软件的组合中实现。

[0021] 内容服务器120是可以托管诸如内容(例如网页)、脚本(例如JavaScript脚本)、服务(例如应用)等等之类的web资源的服务器。内容服务器120可以从订户设备102接收请求数据，处理请求数据，并将响应数据返回到订户设备102。内容服务器120可以是web服务器、企业服务器等。

[0022] 插入数据服务器116是指明的服务器或服务器的负载平衡池，其可以存储插入数据。插入数据服务器116可以是远程服务器(例如内容服务器120之一)，或者它可以被集成

在网关108内。

[0023] 图2是图示图1的示范性系统的实施例的框图。为了简单起见，从图2中省略插入数据服务器116以及网络106和118。在实施例中，网关108包括请求监视器202、响应监视器204、数据插入模块206、设备数据库208、策略规则210和订户简档212。

[0024] 请求监视器202可以是软件程序和/或硬件设备，其从订户设备102接收或拦截请求数据，诸如对特定URI的HTTP请求。如果请求数据包括虚拟域(下面讨论)，则请求监视器202可以用实域替换虚拟域。请求监视器202还可以从HTTP请求中提取报头信息，诸如标识订户设备或从其中发出请求的网页的来源的信息。请求监视器202可以将该信息传递到响应监视器204，要么直接地要么通过将其存储在对请求监视器202和响应监视器204二者可访问的存储器(未示出)中。最后，请求监视器将请求数据传输到内容服务器120。

[0025] 响应监视器204可以是从内容服务器120和插入数据服务器116接收响应数据的软件程序或硬件设备。在接收响应数据之后，响应监视器204可以基于以下讨论的准则来确定附加数据是否应当被插入到响应数据中。如果是这样，则响应监视器204可以将响应数据发送到数据插入模块206，从数据插入模块206接收修改的响应数据，并将修改的响应数据传输到订户设备102。否则，响应监视器204可以将未改变的响应数据重新传输到订户设备102。

[0026] 数据插入模块206可以是软件程序和/或硬件设备，其从响应监视器204接收响应数据，获取插入数据，通过将插入数据添加到响应数据而修改响应数据，并将修改的响应数据传输回到响应监视器204。

[0027] 设备数据库208可以是软件程序和/或硬件设备，其存储关于各种订户设备102的信息。存储的信息例如可以包括特定订户设备102和/或其互联网访问应用104的技术能力。存储的信息还可以指示特定设备是否适合于数据插入，下面进一步描述。

[0028] 策略规则210可以是在软件程序和/或硬件设备中实现的数据库，其存储关于在请求或响应时可以应用的策略行动(诸如下面描述的使能数据插入)的信息。策略规则210还可以存储关于伴随策略行动的条件的信息，诸如适合的订户设备102的列表或适合的网页URI的列表，以及用于应用这些行动所需的变元，诸如要插入的脚本资源的URI。

[0029] 订户简档212可以是在软件程序和/或硬件设备中实现的数据库，其存储关于订户及其数据会话的信息，诸如唯一订户标识符(例如MSISDN或NAI)、当前指派给订户设备102的IP地址和接入点名称(APN)、订阅信息(例如数据计划)、个性化信息(例如订户偏好)等。

[0030] 设备数据库208、策略规则210和订户简档212可以各自与响应监视器204通信，并且可以各自位于要么网关108内，要么在可以与网关108通信的远程服务器上。

[0031] 在示例实施例中，订户正在使用互联网访问应用104并请求特定的网页，例如通过在地址栏中键入请求的网页或通过在另一网页处的超链接上点击。作为响应，互联网访问应用104发出HTTP请求，其包括请求的网页的URI。例如，URI可以具有以下格式：

[0032] http:// [web服务器地址]:[端口]/[网页名称]

[0033] [Web服务器地址]可以是托管请求的网页的内容服务器120的域名(例如“www.wikipedia.com”)或者IP地址(例如“208.80.154.225”)。[网页名称]指示在该内容服务器120上的特定网页的名称，例如“wiki/DNA”。有时，可以从URI中省略[网页名称]，指示正在请求内容服务器120的默认网页。前缀“http://”标识要用来检索网页的通信协议，并

且可以改变为任何其它合适的协议，诸如用于安全网页的“https://”。通信端口由[端口]指示，但是如果要使用用于给定协议的默认端口(例如用于HTTP的端口80)，它也可以被省略。

[0034] 请求监视器202从互联网访问应用104接收HTTP请求，可选地执行虚拟域名替换(以下讨论)，可选地从HTTP请求提取报头信息，并且最后将HTTP请求转发到网络118。如果在HTTP请求中包含的URI是正确的，并且对应于现有内容服务器120上的现有网页，则响应监视器204从该内容服务器120接收包括请求的网页的HTTP响应。网页例如可以是超文本标记语言(“HTML”)文件。HTML是用来描述网页内容的标准语言。

[0035] 响应监视器204可以分析接收的网页，并确定是否需要数据插入。在一些实施例中，为了确定是否需要数据插入，响应监视器204可以标识订户设备102，并通过使用设备数据库208来检查特定的设备或特定类型的设备是否适合于数据插入。例如可以通过从先前由请求监视器202接收的对应HTTP请求的报头信息获得用户-代理(User-Agent)字段而实现标识订户设备。在一些实施例中，对着URI的预定义列表来匹配网页URI，以确定是应当使能(如果URI在“白名单”中)还是禁用(如果URI在“黑名单”中)数据插入。在一些实施例中，确定还可以基于HTTP响应的内容类型。例如，响应监视器204可以决定只有包含HTML页面的HTTP响应可以承受数据插入。在一些实施例中，响应监视器204可以检查策略规则210，以确定对于特定订户、会话或事务是否允许数据插入。在一些实施例中，可以允许订户禁用数据插入，并且响应监视器204可以通过访问订户简档212而确定是否将其禁用。

[0036] 在一些实施例中，在较早的阶段由请求监视器202完成关于是否执行数据插入的确定。因此，在从互联网访问应用104接收HTTP请求之后，请求监视器202可以通过使用上述数据库和方法决定是否要执行数据插入，并将其决定提供给响应监视器204。响应监视器204然后可以简单地通过查看由请求监视器202提供的决定而确定是否要执行数据插入。

[0037] 如果确定了不需要任何数据插入，则响应监视器204向互联网访问应用104提供接收的网页。如果需要数据插入，则响应监视器204向数据插入模块206提供网页，从数据插入模块206接收修改的网页，并将修改的网页转发到互联网访问应用104。不管是否修改网页，互联网访问应用104接收网页，处理它，并将它显示给订户。

[0038] 图3A图示由订户请求的示范性原始网页310。在实施例中，用HTML描述原始网页310。原始网页310可以包括报头区段(包含在标签<head>和</head>之间)，其可以包括HTML元素，诸如网页标题、网页描述、脚本等。原始网页310还可以具有主体区段(包含在标签<body>和</body>之间)，其可以包括HTML元素，诸如文本段落、图像、按钮、到其它网页的超链接等等。

[0039] 在从响应监视器204接收原始网页310时，数据插入模块206可以将插入数据添加到原始网页310。可以将插入数据添加到报头区段、主体区段或文件中的任何其它位置中，优选顺从各种行业标准和/或互联网访问应用104的要求。

[0040] 图3B图示作为将插入数据330插入到原始网页310中的结果所获得的示范性的修改的网页320。在一些实施例中，插入数据330可以包括一个或多个脚本元素，诸如远程脚本元素332或嵌入式脚本元素334。脚本可以是由互联网访问应用104并且优选由行业标准所支持的任何类型或语言。例如，插入数据330可以包括顺从ECMAScript(ECMA-262)的语支之一的脚本，诸如JavaScript、Jscript，或由互联网访问应用所支持的任何其它现有或未来

的脚本语言，诸如VBScript等。添加插入数据330之后，数据插入模块206将修改的网页320传递到响应监视器204，其可以将修改的网页320提供给互联网访问应用104。

[0041] 互联网访问应用104接收修改的网页320，并通过处理其中包含的HTML元素而将其显示给订户。虽然可以立即显示诸如标题、文本和按钮之类的一些HTML元素，但诸如图像之类的其它HTML元素可以包括到远程内容的URI(链接)，其在可以被处理和显示之前必须被检索。为了检索远程内容，互联网访问应用104发出包含其URI的新的HTTP请求。

[0042] 在修改的网页320的处理期间的某点处，互联网访问应用104开始处理插入数据330中包含的元素，例如包括嵌入式脚本元素334和远程脚本元素332。嵌入式脚本元素334包括可以立即由互联网访问应用104执行的脚本的实际内容(由[脚本内容]指示)。相比之下，远程脚本元素332不包括脚本内容；代替地，它包括标识包含脚本本身的资源(文件)的远程位置的URI(被指示为[脚本URI])。因此，在远程脚本元素332的情况下，互联网访问应用104首先通过发出对应HTTP请求而检索脚本文件，等待以从响应监视器204获得脚本文件，并且仅仅那时执行脚本。为了优化的目的，可以预处理(例如由ISP/MNO)脚本文件以最小化其文件大小。例如，可以从脚本文件中移除不必要的内容，诸如空白或注释。此外，可以插入(例如由响应监视器204)HTTP缓存指令，其将指示互联网访问应用104将脚本保持在缓存中达更长的时间段，预计对相同脚本的后续HTTP请求。

[0043] 在一些实施例中，脚本在其执行时可以将附加内容和内容区域添加到修改的网页320。换句话说，脚本可以包括指示互联网访问应用104创建和显示新图形元素的命令。

[0044] 在一些实施例中，脚本可以通过创建新的内联(inline)框架(“iframe”)元素并且例如将其添加到修改的网页320的<body>区段而添加新的内容区域。Iframe允许将来自另一网页的内容插入到现有网页内的矩形框架中。以HTML形式编写，iframe具有下列格式：

[0045] <iframe src=[插入的网页URI]>[备份内容]</iframe>

[0046] 其中[插入的网页URI]指向将在iframe内加载和显示的远程网页，并且[备份内容]包括如果互联网访问应用不支持iframe则将显示的HTML内容。此外，可以定义网页内的iframe的尺寸和位置，如下面将示出的。

[0047] 图4图示用于将包含远程内容的iframe插入到网页中的示范性JavaScript脚本410。JavaScript脚本410可以直接嵌入在嵌入式脚本元素334中，或者其可以被远程托管并且从远程脚本元素332引用，如上所讨论。当互联网访问应用104运行JavaScript脚本410时，其创建新的iframe 412，并将新的iframe添加到修改的网页320的<body>区段418。iframe的大小和位置还由脚本定义(如416所指明)。在指向远程网页(由[插入的网页URI]指示)的“src”属性414中定义要在iframe内显示的内容。结果，互联网访问应用104将经由另一HTTP请求而检索远程网页，并显示iframe内部的远程网页的内容，iframe被放置在所显示的修改的网页320内的预定义位置处。

[0048] 在一些实施例中，JavaScript脚本410可以添加多于一个iframe，并且它还可以包括其它类型的HTML元素。

[0049] 图5A、5B、5C和5D图示其中一个或多个iframe可以被添加到网页的各种示范性的配置。图5A图示示范性的页脚/报头配置，其中报头iframe 512和页脚iframe 514分别被添加在网页的原始内容510的上方和下方。添加的iframe可以被设置以保持在要么相对于网页边界(通过与网页的内容一起滚入和滚出屏幕)要么相对于屏幕边界(通过不滚入和滚出

屏幕)的恒定位置中。

[0050] 图5B图示示范性的叠覆配置,其中添加叠覆iframe 516,以便覆盖网页的原始内容510的一部分。可以设置叠覆iframe 516,以保持在要么相对于网页边界要么相对于屏幕边界的恒定位置中。此外,如果互联网访问应用104和/或订户设备102支持动态视口(即放大和缩小),则叠覆iframe 516可以将其大小调整到缩放水平或者保持大小恒定而不管缩放水平。在一些实施例中,可以添加多于一个叠覆iframe 516。在一些实施例中,叠覆iframe 516可以是半透明的,或者原始内容510可以变暗,以使得叠覆更加突出。

[0051] 图5C图示示范性的侧边栏配置,其中左边栏iframe 518和右边栏iframe 520分别被添加到网页的原始内容510的左边和右边。添加的iframe可以被设置,以保持在要么对网页边界要么相对于屏幕边界的恒定位置中。

[0052] 图5D图示示范性的内联(in-line)配置,其中与网页的原始内容510内联地添加一个或多个iframe 522。添加的iframe 522可以替换原始内容510的一些部分。例如,当网页承载不能由浏览器显示的富互联网应用(RIA)内容(例如Adobe Flash或Microsoft Silverlight)时,嵌入在网页的原始内容510中的这样的内容的一些或全部出现可以用iframe 522内联地替换,所述iframe 522包含由浏览器支持的并且可以显示的基于标准的内容。

[0053] 托管脚本和iframe内容

[0054] 在一些实施例中,插入数据具有两个或更多远程脚本元素332,并且在相同的远程服务器上托管(存储)对应于所有或者至少两个或更多远程脚本元素332的脚本文件。托管脚本文件的远程服务器可以是指明的服务器,诸如插入数据服务器116。作为示例,在插入数据服务器116上托管两个JavaScript文件:“header.js”和“footer.js”,并且插入数据服务器116的IP地址是1.2.3.4。除了其它事物以外,插入数据330于是可以包含下列远程脚本元素332:

[0055] <script src="http://1.2.3.4/header.js"></script>

[0056] <script src="http://1.2.3.4/footer.js"></script>

[0057] 出于许多原因,在相同的服务器上托管脚本可以是有利的,许多原因之一与同源策略有关。同源策略是web安全性概念,其准许源自相同的服务器(托管在相同的服务器上)的文档或脚本访问彼此的方法和属性而没有任何具体的限制,但防止访问跨源自不同服务器的页面的大多数方法和属性。因此,在以上示例中的脚本header.js和footer.js将能够访问彼此的方法和属性,因为它们源自相同的服务器——插入数据服务器116。

[0058] 在一些实施例中,由脚本(例如经由iframe)添加到网页的不同远程内容也源自相同的服务器。也就是说,如果包含若干远程网页的若干iframe被添加到当前网页,则根据一些实施例,可以在相同的服务器上托管若干远程网页。此外,在一些实施例中,在托管脚本本身的相同的服务器上托管远程内容。

[0059] 根据以上讨论的示例,图6图示示范性的插入数据服务器116。在示例中,插入数据服务器116具有1.2.3.4的IP地址,并且托管至少两个脚本文件(header.js和footer.js)和至少两个网页(header.html和footer.html)。脚本header.js添加包含网页“header.html”的iframe,并且脚本footer.js添加包含网页“footer.html”的iframe。脚本在网页的顶部和底部放置iframe,其中通过相应地设置iframe的“顶部”属性而插入iframe(例如修改的

网页320)。

[0060] 在相同的服务器上托管由此插入的脚本和网页实现若干优点。例如,在这种情况下同源策略允许脚本彼此通信,允许插入的网页彼此通信(例如使用W3C HTML5 Web Messaging(消息传递)API),并允许每个脚本与每个插入的网页通信。同时,因为原始网页通常不被托管在与添加的脚本和插入的网页相同的服务器上,原始网页的观感或行为不能由添加的脚本或插入的网页所操纵,并且反之亦然。这给原始和插入的网页二者提供安全性和所有权保护。

[0061] 为了附加的安全性,在一些实施例中,插入数据服务器116的真实地址(域名或者IP地址)不出现在修改的网页上。代替地,当引用在插入数据服务器116上托管的任何元素时,数据插入模块206可以使用预定义的虚拟(例如不存在的)域名。此外,如果由脚本插入的远程内容也托管在插入数据服务器116上,如图6中的示例中那样,脚本还可以通过使用虚拟域名来引用远程内容。例如,如果预定义的虚拟域名被选为“www.virtual-domain.com”,则远程脚本对象334随着它们出现在插入数据330中可以看上去像这样:

[0062] <script src=”http://www.virtual-domain.com/header.js”></script>

[0063] <script src=”http://www.virtual-domain.com/footer.js”></script>

[0064] 并且脚本内的指令可以看上去分别像这样:

[0065] new_iframe.setAttribute(″src″,“http://www.virtual-domain.com/header.html”);

[0066] new_iframe.setAttribute(″src″,“http://www.virtual-domain.com/footer.html”);

[0067] 可以由请求监视器202解析(替换)虚拟域名。请求监视器202接收和分析来自互联网访问应用104的请求数据,诸如HTTP请求。在一些实施例中,请求监视器202可以在请求数据内检测包括预定义的虚拟域名的请求。在检测到预定义的虚拟域名之后,通过用诸如插入数据服务器116之类的预定义的服务器的实域名或IP地址替换预定义的虚拟域名的任何出现,请求监视器202可以修改请求数据。网关108然后将修改的请求数据发送到网络118,网络118根据替换的域名来引导请求。虚拟域名的使用还提供以下灵活性:在不必改变脚本的URI的情况下将脚本重定位到不同的插入数据服务器或服务器池。

[0068] 在一些实施例中,由数据插入模块206插入的远程内容(要么直接地要么经由脚本,如以上所讨论)可以包括Web 服务调用。Web 服务是允许在不同服务器上运行的应用彼此无缝通信的软件技术。例如,在订户设备102上由互联网访问应用104执行的网页可以使用Web 服务,以将数据发送到在远程服务器上运行的应用,并且可以从该应用接收数据。可以通过使用异步JavaScript和XML(“AJAX”)和通过使用XMLHTTPRequest(XMLHTTP请求)(“XHR”)对象来实现Web 服务调用。

[0069] 在一些实施例中,从由脚本插入的iframe中所包括的远程网页发出XHR请求,其中远程网页托管在插入数据服务器116上。在一些实施例中,由于同源策略规则,对除插入数据服务器116以外的服务器的XHR请求不可以由互联网访问应用104允许。在一些实施例中,这可以通过拦截对这样的跨源XHR请求的HTTP响应和向HTTP响应添加报头来克服,所述报头明确地允许来自源自插入数据服务器116的网页的调用。

[0070] 例如,请求监视器202可以标识源自插入的远程网页的HTTP请求,并且响应监视器

204然后可以修改响应于所标识的HTTP请求而接收的HTTP响应的HTTP报头。为了标识源自插入的远程网页的HTTP请求，请求监视器202可以检查所有传入的HTTP请求的HTTP报头，并且例如标识具有简单请求方法(即OPTIONS(选项)、HEAD(头部)、GET(得到)或POST(告示))的所有请求，其报头包括字段“来源”，并且其“来源”字段对应于插入数据服务器116。

[0071] 在标识了源自插入的网页的请求之后，请求监视器202例如可以指示响应监视器204拦截将响应于该请求而接收的HTTP响应。当HTTP响应由响应监视器204拦截时，响应监视器204可以修改HTTP响应，诸如以向互联网访问应用指示：应当允许从插入数据服务器116上托管的网页发出的XHR请求。这例如可以通过将下列W3C跨源资源共享(“CORS”)报头添加到HTTP响应而实现：

[0072] HTTP Request(请求)：

[0073] OPTIONS|HEAD|GET|POST http://... HTTP/1.1

[0074] Origin(来源)：http://[插入数据服务器116地址]:[端口]

[0075] Access-Control-Request-Method(访问-控制-请求-方法)：...

[0076] Access-Control-Request-Headers(访问-控制-请求-报头)：...

[0077] HTTP Response(响应)：

[0078] HTTP/1.1 200 OK

[0079] Access-Control-Allow-Origin(访问-控制-允许-来源)：

[0080] http://[插入数据服务器116地址]：[端口]

[0081] Access-Control-Allow-Methods(访问-控制-允许-方法)：...

[0082] Access-Control-Allow-Headers(访问-控制-允许-报头)：...

[0083] 其中，[插入数据服务器116地址]可以是插入数据服务器116的IP地址或域名(实或虚拟的)。

[0084] 图7是图示web内容和web服务的安全网络内插入的示范性方法的流程图。该方法可以由网关(例如网关108)执行。虽然流程图以特定次序公开下列步骤，但领会的是：适当的地方，可以移动、修改、合并或删除至少一些步骤。

[0085] 方法从订户设备(例如订户设备102)接收(702)请求。然后方法可选地从请求提取(704)报头信息。报头信息例如可以包括关于订户设备的信息以及关于发起请求的网站的来源的信息。接下来，方法可选地解析(706)虚拟域名，通过检测请求是否包括预定义的虚拟域名并用实域名或IP地址替换请求中预定义的虚拟域名的每个出现。然后方法将请求传递(708)到例如网络，诸如网络118。

[0086] 在步骤710处，方法接收对应于传递的请求的响应。响应例如可以包含报头(例如HTTP报头)和网页。然后方法确定(712)是否执行数据插入。该确定可以基于各种因素。例如，方法可以检查特定的设备或特定类型的设备是否适合于数据插入。例如可以通过从在704处提取的报头信息获得用户-代理字段而实现标识订户设备。确定还可以基于响应的内容类型。例如，只有响应是包含HTML网页的HTTP响应的情况下，方法才可以决定执行数据插入。通过访问一个或多个数据库(例如设备数据库208、策略规则210和订户简档212)，方法还可以检查对于特定订户、会话或事务是否允许数据插入。如果方法决定(712)不需要数据插入，则其继续进行到步骤716。否则，方法继续进行到步骤714。

[0087] 在步骤714处，方法将脚本数据插入到响应中所包括的网页中。脚本数据例如可以

被添加到网页的<head>或<body>区段中。脚本可以托管在指明的服务器上(例如在插入数据服务器116上),并且脚本数据可以指示所指明的服务器的名称。在一些实施例中,代替于指示所指明服务器的真实名称,脚本数据可以指示虚拟域名。脚本在其执行时可以将新的内容和内容区域插入到网页中。新的内容区域例如可以是包括远程网页的iframe,其中例如可以在相同的所指明服务器上托管远程网页。在一些实施例中,远程网页可以包括Web服务调用。

[0088] 接下来,方法可以将报头数据插入(716)到响应的报头中。插入的报头数据可以允许来自插入的iframe中所包括的远程网页的跨源Web服务调用。最后,方法可以向订户设备(例如订户设备102)提供(718)响应。

[0089] 本文公开的方法可以被实现为计算机程序产品,即在信息载体中(例如在机器可读存储设备中)有形地体现的计算机程序,以供由数据处理装置执行或控制数据处理装置的操作,所述数据处理装置例如可编程处理器、计算机或多个计算机。计算机程序可以用任何形式的编程语言编写,包括编译或解译的语言,并且可以以任何形式部署它,包括作为独立的程序或作为模块、组件、子例程或适合于在计算环境中使用的其它单元。可以部署计算机程序以在一个站点处的一个计算机上或多个计算机上执行,或者跨多个站点分布并通过通信网络互连。

[0090] 本文公开的方法的一部分或全部还可以由专用集成电路(ASIC)、现场可编程门阵列(FPGA)、复杂可编程逻辑器件(CPLD)、印刷电路板(PCB)、数字信号处理器(DSP)、可编程逻辑组件和可编程互连的组合、单个中央处理单元(CPU)芯片、在母板上组合的CPU芯片、通用计算机或者能够执行本文公开的web内容和web服务的安全网络内插入的设备或模块的任何其它组合来实现。

[0091] 在前面的说明书中,已经参考具体的示范性实施例描述了主题。然而,将明显的是:可以做出各种修改和改变而不脱离如在随后的权利要求中阐述的主题的更广泛的精神和范围。说明书和附图因此被视为说明性的而不是限制性的。考虑到本文公开的发明的说明书和实践,其它实施例对于本领域技术人员可以显而易见。

[0092] 根据MICRO2-08号合同,导致本文公开的主题的开发的工作由Hellenic Funds(希腊基金)和由European Regional Development Fund(欧洲地区发展基金)(ERDF)在Hellenic National Strategic Reference Framework(希腊国家策略参考框架)(ESPA)2007-2013下共同资助的。

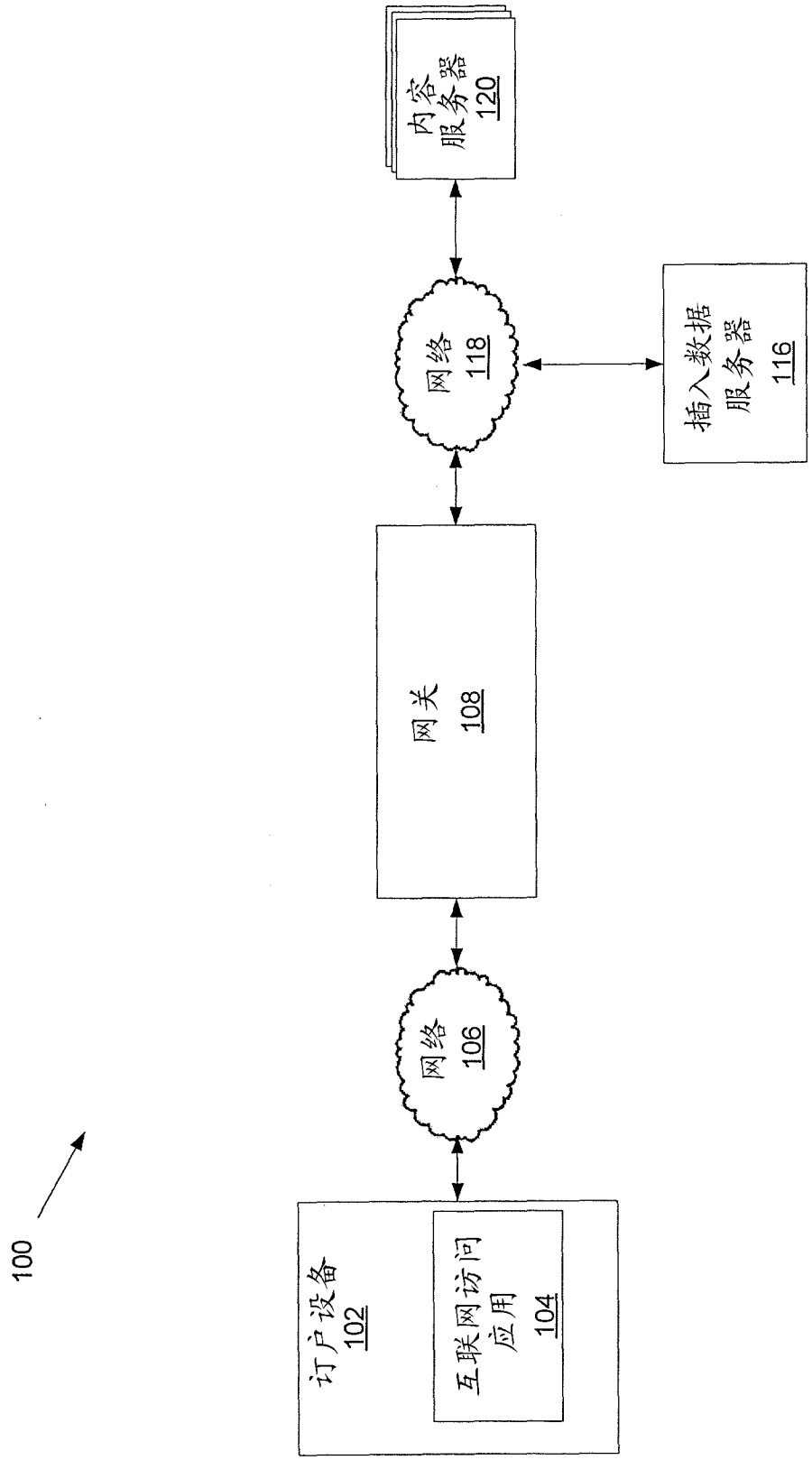

100
订户设备
102
互联网访问
应用
104
网络
106
网关
108
网络
118
内容
服务器
120
插入数据
服务器
116

图 1

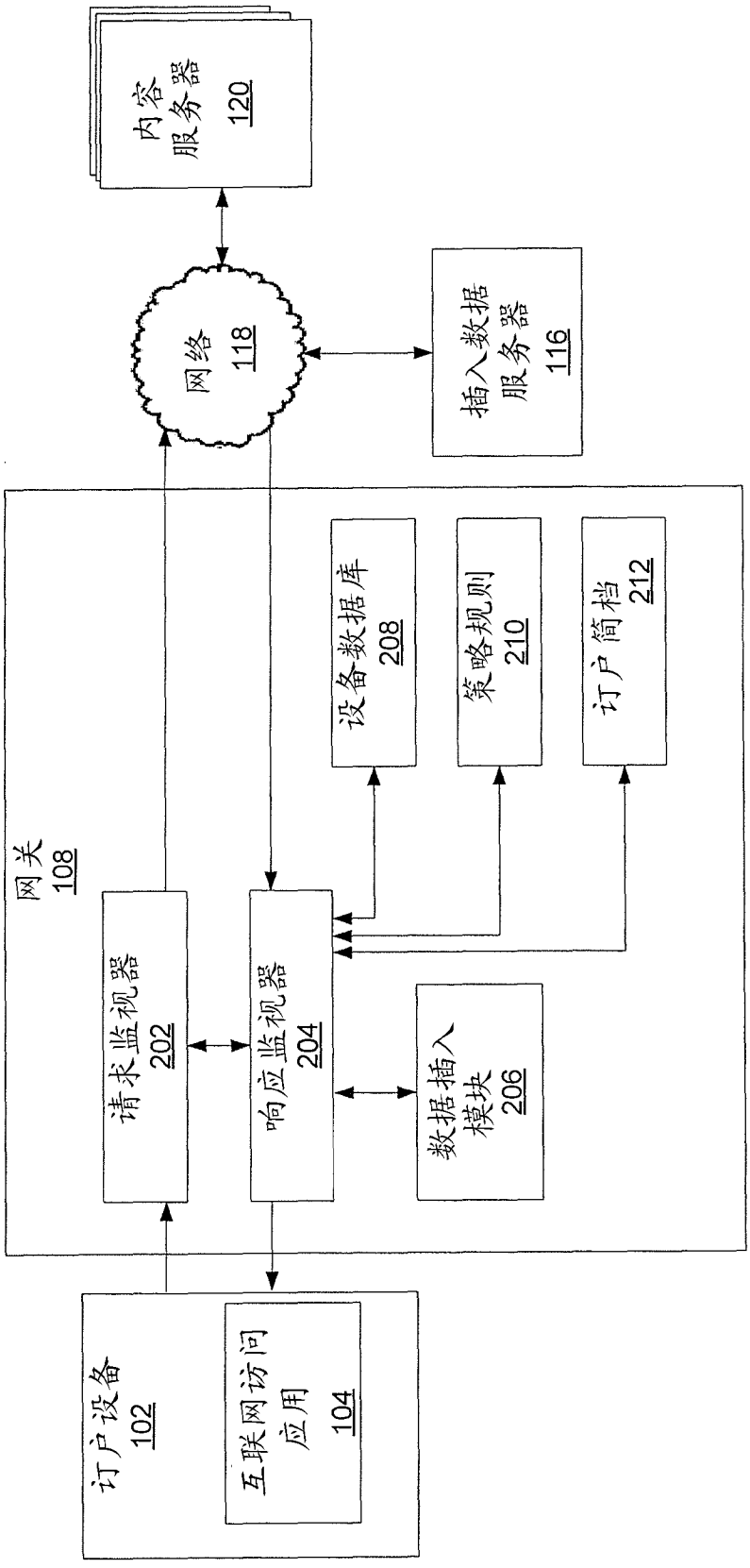
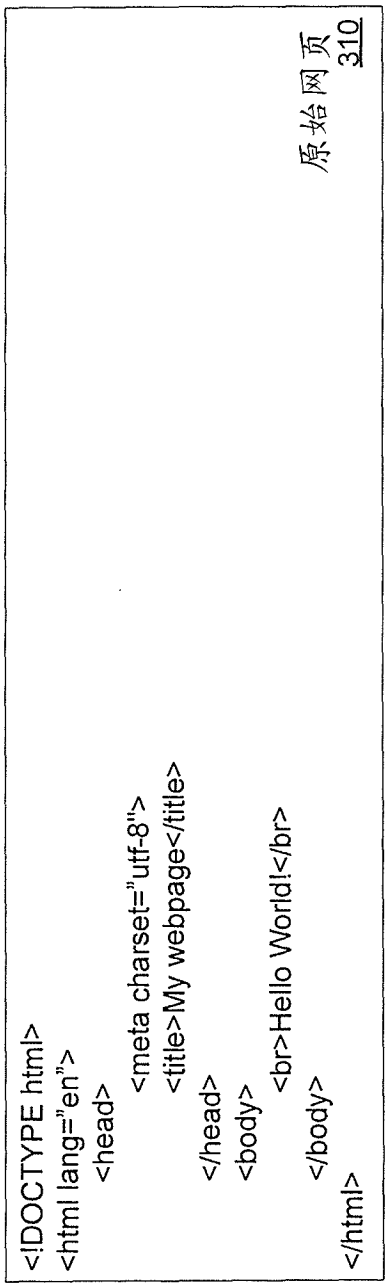
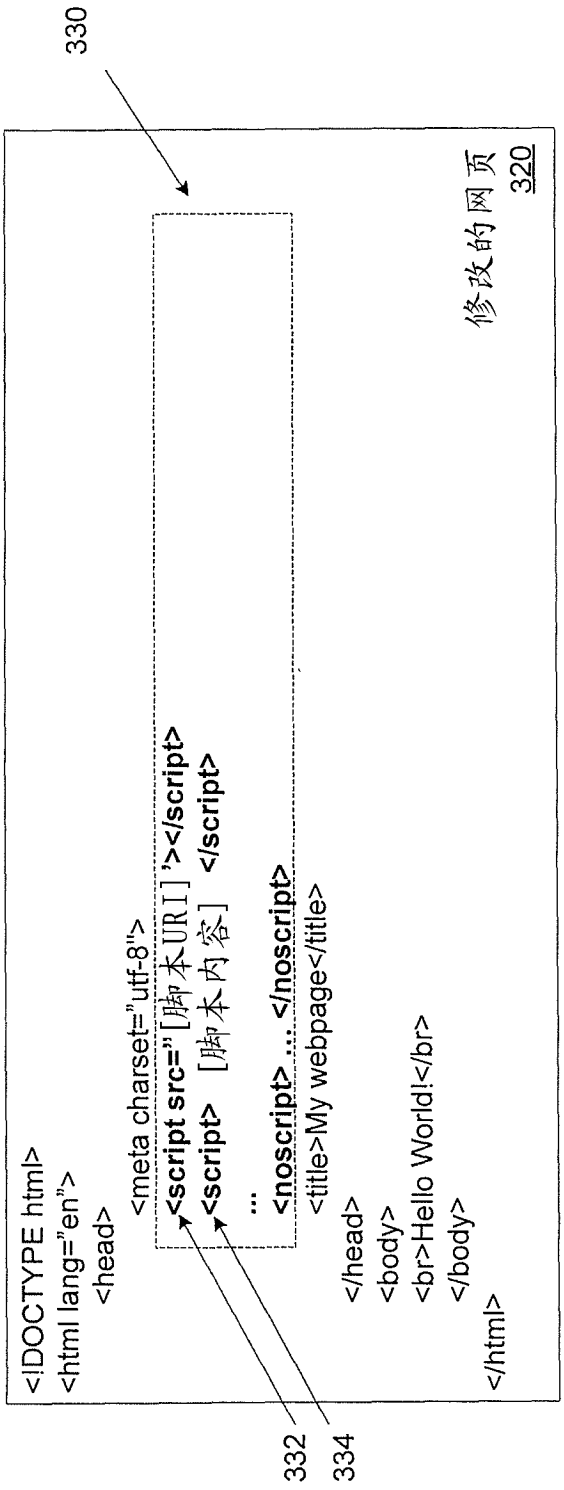

内容服务器 120
网络 118
插入数据服务器 116
网关 108
设备数据库 208
策略规则 210
订户简档 212
请求监视器 202
响应监视器 204
数据插入模块 206
订户设备 102
互联网访问应用 104

图 2


原始网页
310
<!DOCTYPE html>
<html lang="en">
<head>
<meta charset="utf-8">
<title>My webpage</title>
</head>
<body>

Hello World!</br>
</body>
</html>

图 3A


330
修改的网页
320
<!DOCTYPE html>
<html lang="en">
<head>
<meta charset="utf-8">
<script src="[脚本URI]"></script>
<script> [脚本内容] </script>
...
<noscript> .... </noscript>
<title>My webpage</title>
</head>
<body>

Hello World!</br>
</body>
</html>
332
334

图 3B

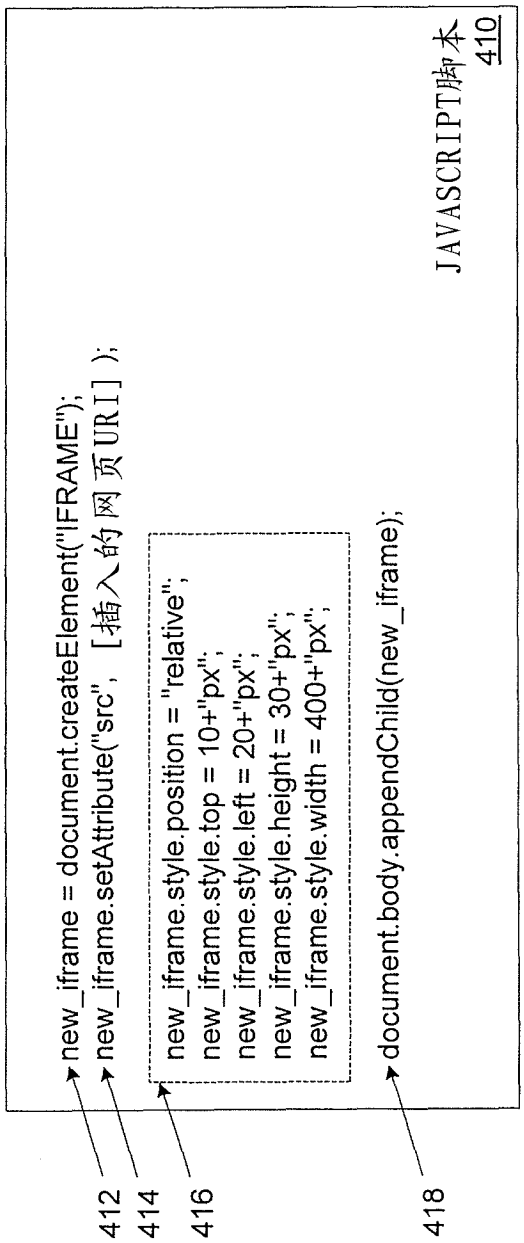

JAVASCRIPT脚本
410
new_iframe = document.createElement("IFRAME");
new_iframe.setAttribute("src", [插入的网页URI]);
new_iframe.style.position = "relative";
new_iframe.style.top = 10+"px";
new_iframe.style.left = 20+"px";
new_iframe.style.height = 30+"px";
new_iframe.style.width = 400+"px";
document.body.appendChild(new_iframe);
412
414
416
418

图 4

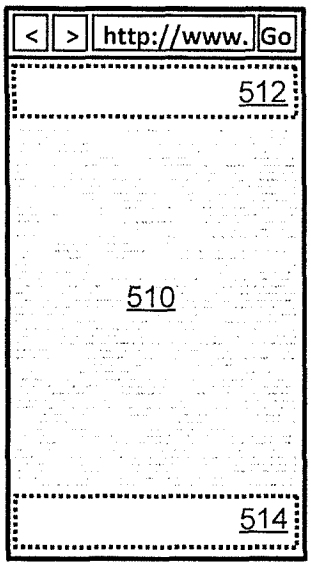


图 5A

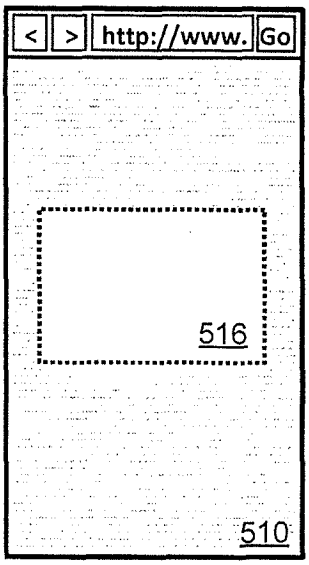


图 5B

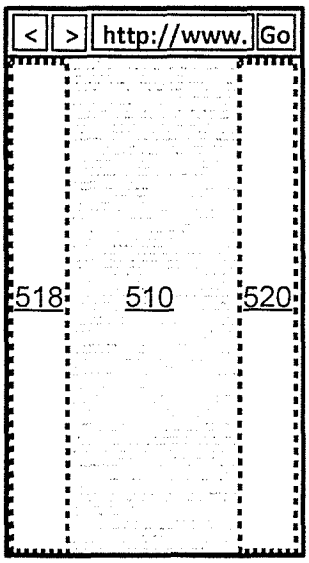


图 5C

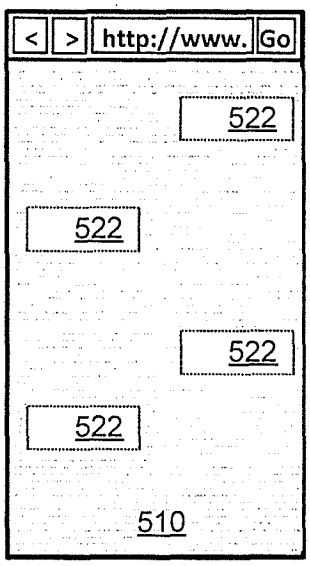
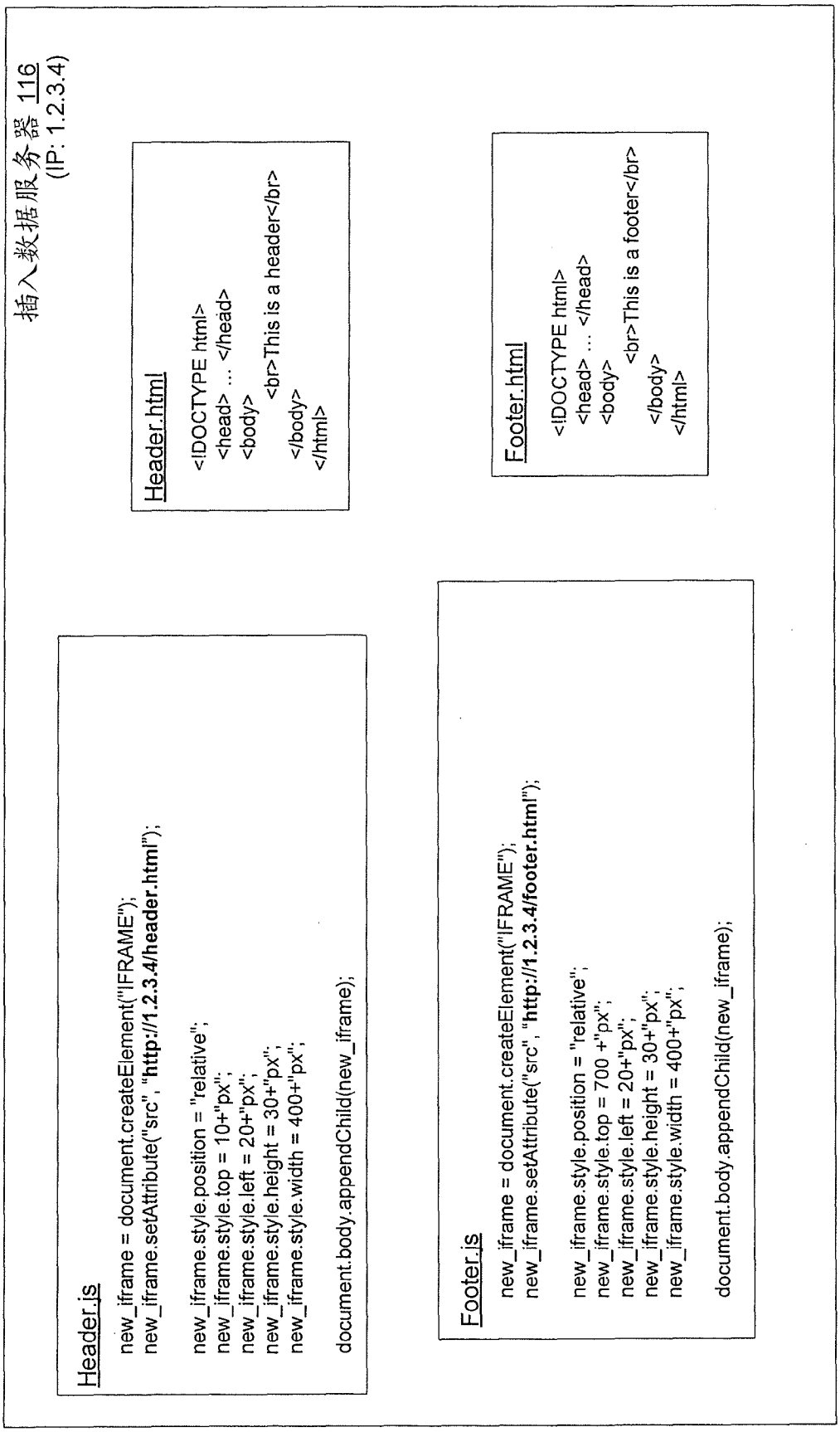


图 5D


插入数据服务器 116
(IP: 1.2.3.4)
Header.is
new_iframe = document.createElement("IFRAME");
new_iframe.setAttribute("src", "http://1.2.3.4/header.html");
new_iframe.style.position = "relative";
new_iframe.style.top = 10+"px";
new_iframe.style.left = 20+"px";
new_iframe.style.height = 30+"px";
new_iframe.style.width = 400+"px";
document.body.appendChild(new_iframe);
Header.html
<!DOCTYPE html>
<head> ... </head>
<body>

This is a header</br>
</body>
</html>
Footer.is
new_iframe = document.createElement("IFRAME");
new_iframe.setAttribute("src", "http://1.2.3.4/footer.html");
new_iframe.style.position = "relative";
new_iframe.style.top = 700 +"px";
new_iframe.style.left = 20+"px";
new_iframe.style.height = 30+"px";
new_iframe.style.width = 400+"px";
document.body.appendChild(new_iframe);
Footer.html
<!DOCTYPE html>
<head> ... </head>
<body>

This is a footer</br>
</body>
</html>

图 6

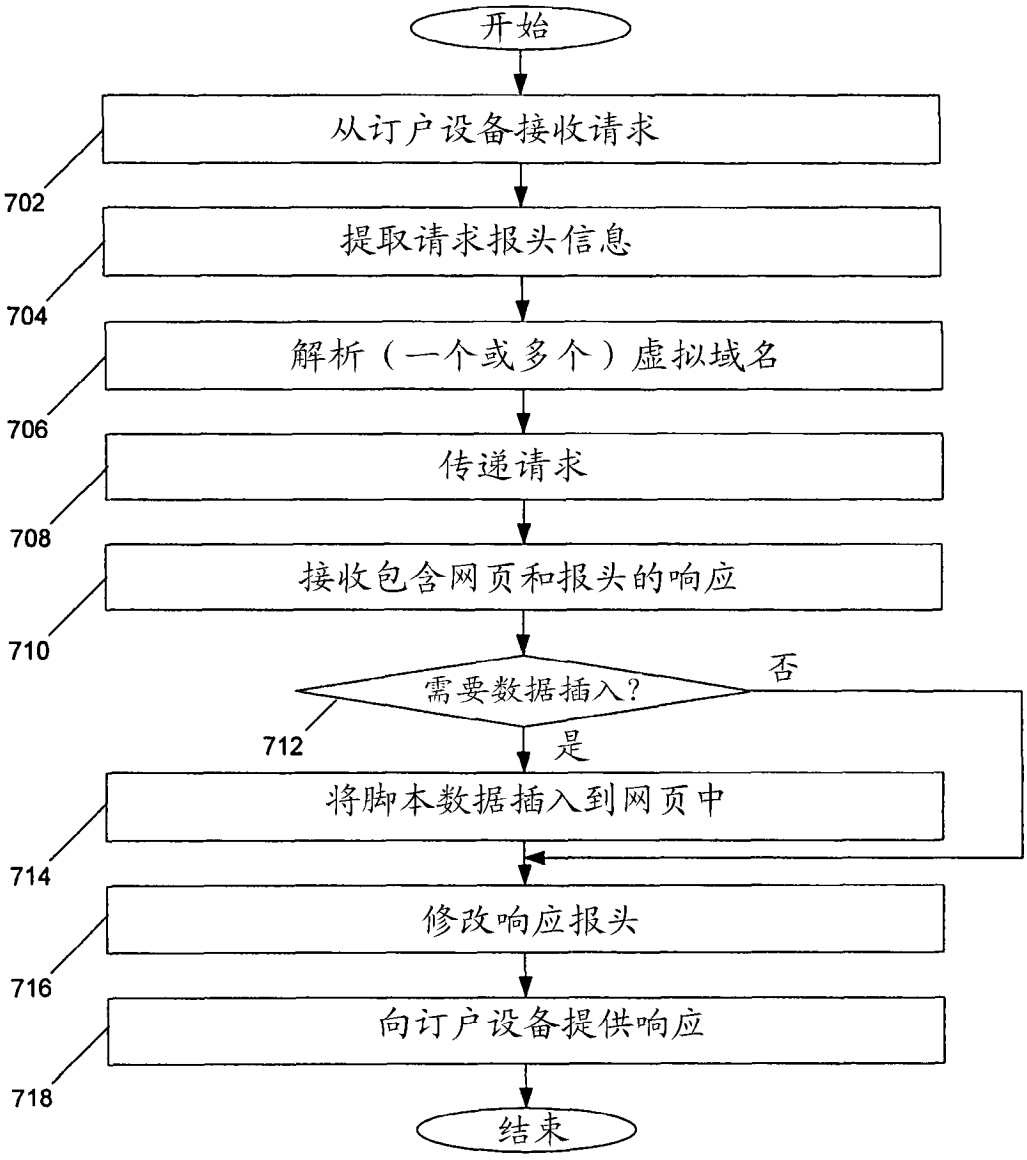

开始
从订户设备接收请求
702
提取请求报头信息
704
解析（一个或多个）虚拟域名
706
传递请求
708
接收包含网页和报头的响应
710
需要数据插入?
712
否
是
将脚本数据插入到网页中
714
修改响应报头
716
向订户设备提供响应
718
结束

图 7