[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
H04L 9/00

[12] 发明专利说明书

专利号 ZL 98814246.5

[45] 授权公告日 2005 年 11 月 16 日

[11] 授权公告号 CN 1227858C

[22] 申请日 1998.8.21 [21] 申请号 98814246.5
[86] 国际申请 PCT/US1998/017410 1998.8.21
[87] 国际公布 WO2000/011832 英 2000.3.2
[85] 进入国家阶段日期 2001.3.21
[71] 专利权人 维斯托公司
地址 美国加利福尼亚
[72] 发明人 马克·D·里金斯
审查员 范晓寒

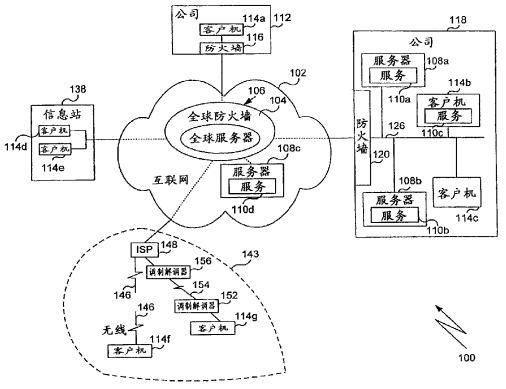
[74] 专利代理机构 中国国际贸易促进委员会专利商标事务所
代理人 杨国旭

权利要求书 3 页 说明书 13 页 附图 10 页

[54] 发明名称 实现对计算机网络中服务的安全访问的系统和方法

[57] 摘要

全球服务器(106)包括一个用于建立与客户机通信联络的通信引擎；与确定客户机特权的通信引擎相连接的安全装置；与安全装置连接的小服务程序主机引擎，用于基于户特权、为客户机(114a)提供一个应用小程序，此程序实现与安全服务(110a)间的输入/输出。 以及一个密钥保存，用于存储使得客户机能够访问安全服务的密匙。 全球服务器可以与多个站点连接，其中每一个站点提供多种服务。 每一个站点都可以通过防火墙(116)而被保护。 相应地，全球服务器存储密匙，经由防火墙(116)实现与服务(110a)的通信。



ISSN1008-4274

1. 一种用于允许客户访问安全服务的系统，所述系统包括：

一个通信引擎，用于建立与客户机的通信链路；

与所述通信引擎相连接的、用于确定客户机特权的安全装置；

一个与安全装置连接的小服务程序主机引擎，用于基于客户机特权为客户机提供一个应用小程序，所述应用小程序能实现与所述安全服务之间的输入/输出操作；以及

一个密钥保存装置，用于存储使得客户机能够访问安全服务的密匙。

2. 按照权利要求 1 所述的系统，其中，通信引擎利用 SSL 技术建立与客户机相联系的安全通信。

3. 按照权利要求 1 所述的系统，其中，通信引擎协商用于与客户机交换信息的加密协议。

4. 按照权利要求 1 所述的系统，其中，为与客户机交换信息，通信引擎利用公用密钥进行鉴定。

5. 按照权利要求 1 所述的系统，其中，安全装置利用公用密钥证书来认证客户机。

6. 按照权利要求 1 所述的系统，其中，为确定客户机特权，安全装置检查客户机身份以及认证的级别。

7. 按照权利要求 1 所述的系统，其中，为认证客户机，安全装置检查一本全球证书。

8. 按照权利要求 1 所述的系统，其中，安全装置利用数字签名技术来认证客户机。

9. 按照权利要求 1 所述的系统，其中，小服务程序主机引擎传送一个安全应用小程序给客户机，以使得客户机能够通过此安全装置执行一个认可的安全协议。

10. 按照权利要求 1 所述的系统，其中，服务是通过共同的防火墙保证安全的，并且密匙的配置实现了通过防火墙进行的通信。

11. 按照权利要求 1 所述的系统，进一步包括保护系统的全球防火墙。

12. 按照权利要求 1 所述的系统，进一步包括一个识别安全服务站点的服务地址。

13. 按照权利要求 1 所述的系统，其中，应用小程序为客户机提供与安全服务的定向连接。

14. 按照权利要求 1 所述的系统，进一步包括一个与所述安全服务联系的代理，并且其中，应用小程序使得系统与代理之间能够进行输入/输出。

15. 一种用于使客户机访问安全服务的方法，所述方法包括以下步骤:

使用通信引擎建立与客户机的通信链路;

使用安全装置确定客户机特权;

使用小服务程序主机引擎，基于客户机特权，为客户机提供一个应用小程序，所述应用小程序实现与所述安全服务之间的输入/输出;

从密钥保存装置检索使得客户机能够访问所述安全服务的密匙。

16. 按照权利要求 15 的方法，其中，建立通信链路包括利用 SSL 技术建立与客户机间安全通信的步骤。

17. 按照权利要求 15 的方法，其中，建立通信链路包括为与客户机交换信息而商谈加密协议的步骤。

18. 按照权利要求 15 的方法，其中，建立通信链路包括为与客户机交换信息而利用公用密钥证书的步骤。

19. 按照权利要求 15 的方法，其中，确定客户机特权包括利用公用密钥证书认证客户机的步骤。

20. 按照权利要求 15 的方法，其中，确定客户机特权包括为确定客户机特权而检查客户机身份和认证级别的步骤。

21. 按照权利要求 15 的方法，其中，其中客户机特权包括为认证客户机而检查全球证书的步骤。

22. 按照权利要求 15 的方法，其中，确定客户机特权包括为认证

客户机而利用数字签名技术的步骤。

23. 按照权利要求 15 的方法，其中，建立通信链路包括为了客户机能够执行认可的安全协议而给客户机传送小的安全应用程序。

24. 按照权利要求 15 的方法，进一步包括以下步骤：通过防火墙利用密匙传送安全服务。

25. 按照权利要求 15 的方法，其中，此方法是通过全球服务器执行的，并且它进一步包含了利用全球防火墙保护全球服务器。

26. 按照权利要求 15 的方法，进一步包括一个识别安全服务站点的服务地址。

27. 按照权利要求 15 的方法，其中，包括为客户机提供与安全服务的定向连接的步骤。

28. 按照权利要求 15 的方法，进一步包括利用与安全服务联系的代理，并且其中，应用小程序使得系统与代理之间能够进行输入/输出。

29. 一种用于允许客户机访问安全服务的系统，所述系统包括：

用于建立与客户机的通信链路的装置；

用于确定客户机特权的装置；

基于客户机特权、为客户机提供应用小程序的装置，所述应用小程序实现与安全服务之间的输入/输出；

用于检索使得客户机能够访问安全服务的密匙的装置；

实现对计算机网络中服务的安全访问的系统和方法

技术领域

本发明一般涉及到计算机网络，更具体地说涉及到实现对计算机网络中服务的安全访问的系统和方法。

背景技术

在初期，互联网提供了面向研究的环境，用户和主机对那里的信息的自由、开放式的交换很感兴趣，并且在那里用户和主机相互信赖。然而，互联网络戏剧性地增长，目前大约有 100,000 互相连接的计算机网络和几百万用户。由于互联网络的规模和公开性，它变成了数据盗窃、数据蚀变和其它恶作剧的目标。

事实上，在互联网上的每个人都是有弱点的。在连接之前，公司会权衡互联网连接与安全性损失的利弊。当前的安全技术用来提供客户机和服务器认证、数据机密性、系统完整性以及系统访问控制等。

当前的安全技术中最流行的是防火墙，它包括在可信赖的网络和互联网之间安置的一个中间系统。为避免可信赖网络和互联网之间未经认证的通信，防火墙提供了安全性能的外部参数。一个防火墙可以包括屏蔽路由器、代理服务器和应用层网关。

为了能够访问可信赖的网络中受到保护的服务，互联网上的用户需要用某种方法，例如输入口令、或者利用硬件令牌完成对于询问的回答，向防火墙提供身份。 通过适当的认证，用户可以通过防火墙进入局域网络，但是它通常被限制在预定的服务设置之内，例如电子邮件、FTP（文件传输协议）等等。

一些局域网络管理员只是将服务器放置在防火墙之外，该服务器经常被称为“献身的羔羊”，该服务器存储那些可以被远程用户很容易访问的非机密数据，因而具有很少的安全性能。

一个非军事化区域、或 DMZ，处于用来保护可信赖网络的两个防火墙之间。在 DMZ 中，外部防火墙在允许超级文本传送协议(HTTP)

请求的同时保护服务器免受外部威胁。如果在 DMZ 中一个服务器受到危害，内部防火墙就会保护可信赖的网络。许多公司利用 DMZ 来维护它们的网络服务器。

另一种保护计算机网络的安全技术是公用密钥证书的发行和使用。证书机构把公用密钥证书发布给用户，并且通过某一方法使用户的身份生效、并且发布一个描述用户姓名和公用密钥的证书。作为可靠性的证据，利用本人的私用密匙，该证书机构用计数法标记用户的证书。

这样，当用户经由一台客户计算机连接到一台服务器上时，这台客户计算机就会和服务器交换公用密钥证书。通过利用证书机构的公用密钥来检验证书的署名，每一个用户都会检验该接收证书的可靠性。接着，通过用服务器公用密钥加密信息，用户能够给服务器发送安全的通信链路，并且用用户公用密钥加密信息，服务器能够给用户发送安全通信链路。虽然任何用户可以给出一个公用密钥证书，但是仅有该真实用户和该真实主机才拥有解密信息所需的相应私用密匙。认证和密钥分配的计算机安全系统的实例包括由麻省理工学院开发的 KerberosTM 安全系统和由 IBM 公司开发的 NetSPTM 安全系统。

这些安全技术无法解决与漫游(移动的)用户相关的问题。对于漫游用户来说，维护识别和认证信息例如口令、证书、密钥等等是一个烦琐的处理过程。另外，访问多机系统要求多个密钥，这经常使得跟踪和利用变得过于复杂。而且对防火墙之后的系统的直接访问会危害到安全性能。因此，容易、安全地对计算机服务实现远端访问的系统和方法是必需的。

发明内容

本发明提供一种实现对计算机网络中服务的安全访问的系统和方法。 此网络系统包括一个全球服务器，经由一个计算机网络与计算机服务器连接。全球服务器包括一个通信引擎，用于建立与客户机的通信链路；安全装置，用于与确定客户机特权的通信引擎连接；一个与安全装置连接的小服务程序(servlet)主机引擎，基于客户机特权给客户机提供一个应用小程序，此程序使得客户机与安全服务之间能够进行

输入/输出操作；以及一个密钥保存(文件)，用于存储使得能够对安全服务进行访问的密匙。全球服务器可以与多个站点连接，其中每一个站点提供多种服务。每一个站点都可以被防火墙保护。相应地，全球服务器存储此密匙，用于通过防火墙与服务进行通信。

此方法包括下列步骤：与客户机建立通信链路；识别和认证客户机；确定客户机特权；基于客户机特权，提供一个应用小程序给客户机，此程序使得客户机与安全服务之间能够进行输入/输出操作；检索使访问安全服务密匙；

本发明的系统和方法更好地提供了全球可访问的可信赖的第三方，即全球服务器。该可信赖的第三方安全地存储密匙，起着单一的识别和认证服务的作用。其它系统可以通过全球服务器被访问。全球服务器使用存储的密匙认证某一身份下的用户，此身份被另一系统的现有安全服务所领会，并建立起与所需服务之间的安全通信通道。由于全球防火墙，全球服务器很显著地被保护，以免受外部威胁。 相应地，通过与服务相连接的防火墙，全球服务器为经过认证的客户机提供安全通信。全球服务器可以提供多级别的识别和认证服务。相应地，基于用户状态、识别与认证的强度以及通信通道的保密性，全球服务器可以提供多级别的资源访问。

由于全球防火墙以及由全球服务器执行的识别和认证服务，公司能够在全球服务器上存储相对机密的信息，用于供经认证的客户机使用。 然而，本发明使得公司在全球服务器仅能保持它们的一部分机密信息，这样这个有限的损失就可以由可信赖的第三方系统妥协处理。此外，全球服务器可以很方便地起到客户机代理的作用，用于控制对服务的访问、记录密匙的使用以及对记录资源的访问。

附图说明

图 1 是一个方框图，图示了一个按照本发明的漫游用户网络访问系统；

图 2 是一个方框图，图示了图 1 所示的一例客户机的细节；

图 3 是一个方框图，图示了图 1 所示的全球服务器的细节；

图 4 是一个方框图，图示了图 1 所示的一例服务器的细节；

图 5 是一个流程图，图示了一种用于远程访问一个安全服务的方法；

图 6 是一个流程图，图示了在客户机和全球服务器之间产生连接的图 5 所示的步骤的细节；

图 7 图示了一个示例性的网页；

图 8A 是一个流程图，按照第一实施例图示了图 5 所示的访问服务步骤的细节；

图 8B 是一个流程图，按照第二实施例图示了图 5 所示的访问服务步骤的细节；

图 8C 是一个流程图，按照第三实施例图示了图 5 所示的访问服务步骤的细节；

具体实施方式

图 1 是一个方框图，图示了一个按照本发明的示例性漫游用户网络访问系统 100。系统 100 包括一个计算机互连网络，在这里是指互联网 102。系统 100 另外包括第一公司网络 112、第二公司网络 118、一个信息站（kiosk）网络 138 和一个网络服务提供商(ISP)网络 143，每一个网络都被连接到互联网上。

公司网络 112 包括一个防火墙 116，连接在互联网 102 和客户计算机 114a 之间。公司网络 118 包括一个防火墙，连接在互联网 102 和内部网络信号总线 126 之间。公司网络 118 另外包括：第一个服务器 108a，用于提供第一服务 110a；第二服务器 108b，用于提供第二服务 110b；一个客户计算机 114b，用于存储提供第三服务 110c 的程序；以及一个第二客户计算机 114c；并且每一个都被连接到信号总线 126。这些服务 110a-110d 包括一个电子邮件服务程序、一个地址簿服务程序、一个日历服务程序、一个页面调度服务程序以及一个公司数据库服务程序。

信息站网络 138 包括第一客户计算机 114d 以及第二客户计算机 114e，并且每一个都被连接到互联网 102 上。ISP 网络 143 包括一个 ISP148，它通过无线电通道 146 连接到第一客户计算机 114f 上，并且通过调制解调器 152、156 以及传输线 154 连接到第二客户计算机 114g 上。

互联网 102 包括一个被全球防火墙 104 保护的全球服务器 106，并且还包括一个用于提供服务 110d 的服务器 108e。 客户计算机 114a-114g 和服务 110a-110d 之间的内部通信是经由全球服务器 106 完成的。例如，如果客户计算机 114a-114g 的任何一个用户想访问服务 110a-110d(此服务被提供在系统 100 内用户未知的站点)，那么他就可以利用一个已知的统一资源定位符(URL)来访问由全球服务器 106 提供的网页。 一个示例性的网页 300 在图 7 中被显示、描述。全球防火墙 104 保护全球服务器 106 免受外部威胁。

在获得对全球服务器 106 提供的功能的访问特权之前，用户必须首先获得全球服务器 106 的授权。 获得授权通常要求进行用户识别和认证，例如利用公用密匙证书。一旦进行了认证，全球服务器 106 为用户提供对服务 110a-110d 的访问。应该理解，基于识别和认证的变化强度、以及通信通道的保密性，用户将被授与对服务 110a-110d 访问的变化级别。

为使用户能够访问并控制服务 110a-110d，全球服务器 106 可以在分布式网络环境中使用常规的应用小程序、小服务程序（servlets）或者代理服务器，比如由 Netscape 公司提供的 JavaTM 分布式环境。全球服务器 106 为用户的客户机提供对服务 110a-110d 的访问和控制。全球服务器 106 可以通过对用户的客户机重定向来访问服务 110a-110d 本身；全球服务器 106 可以访问服务 110a-110d 本身并通过代理给客户机提供输入/输出；或者全球服务器 106 可以提供服务 110a-110d 本身。参考图 8A-8C，将描述对服务 110a-110d 不同的三种访问模式。

全球服务器 106 保存所有服务 110a-110d 的网络地址、用户的公用和私人密匙、用户的帐户编号、以及防火墙认证信息等等。防火墙认证信息包括必要的识别、口令和传送防火墙 116 和 120 需要的证书。相应地，用户仅需要保存全球服务器 106 的 URL、以及识别和认证信息，比如一个口令或者用于可使用全球服务器 106 功能的硬件标记。这样，这个漫游用户可以通过任何连接到互联网 102 的计算机终端，能够访问计算机服务 110a-110d。

图 2 是一个方框图，图示了客户计算机 114 的细节，其中客户机 114a-114d 的每一个都是客户机 114 的一种情况。客户机 114 包括一个中央处理器(CPU)210，比如一个摩托罗拉 PC 微处理器或者英特尔奔腾微处理器。一个输入设备 220（例如键盘以及鼠标）以及一个输出装置 230（比如阴极射线管(CRT)显示器），经由信号总线 240 连接到 CPU210。一个通信接口 250、一个数据存储装置 260（例如只读存储器芯片(ROM)或者磁盘）、以及一个随机存取存储器(RAM) 270，经由信号总线 240 也被连接到 CPU210。客户计算机 114 的通信接口 250，如图 1 所示被连接到互联网 102，并且将参考图 1 描述。

操作系统 280，包括用于控制 CPU210 处理过程的程序，并且它通常被存储在数据存储装置 260 中、并装入 RAM270 中用于执行。操作系统 280 包括一个通信引擎 282，用于产生信息数据包并经由通信接口 250 将它们传送到互联网 106 或从互联网接收信息数据包。

操作系统 280 进一步包括一个互联网引擎，比如一个网页浏览器 284，例如由网景公司提供的 NetscapeTM 网页浏览器或者由微软公司提供的 IE 浏览器。网页浏览器 284 包括一个用公用和私用密匙加密信息的加密引擎 285，和一个应用小程序引擎 286，用于执行从全球服务器 106 下载的应用小程序，使得客户机能够访问计算机服务 110a-110d。下载的应用小程序 288 可以包括安全应用小程序 290，用于执行服务例如用户识别和认证、信息完整性服务、以及证书检验。浏览器 284 进一步接收网页数据(391、图 3)、配置数据 390 和识别一组用来选择服务 110a-110d 的信息，并且利用此信息来显示此网页(700、图 7)。此网页浏览器 284 使得用户能够通过客户机 114a-114b 选择地执行服务 110a-110d 中的一种。

应该理解，客户机 114a-114g 例如客户机 114b 可以包括一个服务引擎 490(图 4)，用于提供服务 110a-110d 例如服务 110c。这样，对于一个客户机 114b 的用户，在不知道客户机 114b 提供服务 110c 的情况下，经由全球服务器 106 请求对服务 110c 的访问是有可能的。相应地，全球服务器 106 将为客户机 114 提供一个应用小程序 288，目

的是为用户提供回到客户机 114b 的服务 110c 的接口输入/输出。

图 3 是一个方框图，图示了全球服务器 106 的细节，此服务器包括一个 CPU310 例如一个摩托罗拉 PC 微处理器、或者一个英特尔奔腾微处理器。一个输入设备 320 例如键盘和鼠标、以及一个输出装置 330 例如一个 CRT 显示器通过信号总线 340，被连接到 CPU310 上。一个通信接口 350、一个数据存储装置 360 例如只读存储器或者磁盘、以及一个 RAM370，经由信号总线 340 也被连接到 CPU310。通信接口 350 照惯例作为互联网 102 的一部分被连接到客户机 114。应该理解，虽然全球服务器 106 被描述为单一计算机，但它可以被理解为同时包括构成网络的多个计算机。

操作系统 380，包括用于控制 CPU310 处理过程的程序，并且通常被存储在数据存储装置 260 上、并且被装入 RAM370 中用于执行。操作系统 380 包括一个通信引擎 382 用于产生信息数据包、并且经由通信接口 350 与客户计算机 114 交换信息数据包。

操作系统 380 进一步包括作为全球防火墙一部分的安全服务 384，用于开放与用户通信的通道。例如，当一个客户机试图访问全球服务器 106 时，此安全服务 384 首先确定全球服务器 106 是否从特定端口（没有显示）接收了进入的（in-bound）通信，并且在下面描述的小服务程序主机引擎 386 中确定连接到该特定端口是否经过了认证。假如是的话，经由该特定端口，安全服务 384 就会允许通信引擎 382 开放到客户机 114a-114b 的通信通道。否则，将不开放通道。

操作系统 380 更进一步包括一个网页引擎 387，它基于用户的识别、用户认证的强度以及通信信道的保密性，把网页数据 391 和识别一组可用服务 110a-110d 的信息传送到客户机 114a-114g。一个示例性的网页 700 被显示在图 7 中，并且参考图 7 被描述。网页引擎 387 使得用户能够从网页 700 中选择服务 110a-110d。

网页引擎 387 包括一个小服务程序主机引擎 286，它能把包括一个认证应用小程序（没有显示）的安全应用小程序 290 下载到客户计算机 114 上，并且相应地执行小服务程序 398 的认证小服务程序 397，

以完成识别和认证服务。 认证应用小程序 290 提示用户输入识别和认证信息，然后把此信息传达到认证小服务程序 397。 认证小服务程序 397 检验信息是否正确。 应该理解，用户的认证信息不一定被送到认证小服务程序 397，而是要用一种安全方法例如一个安全混杂来证明它的存在和正确性。 小服务程序主机引擎 386 更进一步包括一个安全通信引擎 396，它可以利用公用密钥证书与客户计算机 114 商讨安全通信通道。

相对于服务 110a-110d 的一个选择，小服务程序主机引擎 386 下载相应的应用小程序 388、相应的配置数据 390 以及相应的用户数据 392，并且可以把相应的服务地址信息 394 下载到客户计算机 114。配置数据 390 包括用于配置用户网页浏览器 284 的信息、用于配置下载的应用小程序 288 的信息、以及用于配置选中的服务 110a-110d 的信息。用户数据 392 可以包括用户和服务所特定的信息，例如存储的书签、日历数据、寻呼机编号等等，此信息被特意地存储在全球服务器 106 上，以便可以容易地存取。服务地址信息 394 识别服务 110a-110d 的站点，这些服务是由全球服务器 106 提供给系统 100 的。 客户计算机 114 执行下载的相应的应用小程序 288，此程序经由小服务程序主机引擎 386(可能使用一个相应的小服务程序 398)使得用户能够访问并控制其相应的服务 110a-110d。可下载的应用小程序 388、配置数据 390、用户数据 392 以及服务地址信息 394 可以被存储在此数据存储设备 360 中。

密钥保存 395 是一个数据文件，用于存储每一个用户的认证信息、公用以及私用的密匙、每一个防火墙的口令信息等等。密钥保存 395 以链表格式组织，这样，基于选中的服务 110a-110d，全球服务器 106 能够检索适当的防火墙口令信息、适当的用户认证信息以及密匙等等。密钥保存 395 可以被存储在数据存储装置 360 上。

图 4 是一个方框图，图示了服务器 108 的细节，这样服务器 108a-108c 和客户机 114b 分别是服务器 108 的不同实例。 服务器 108 包括一个 CPU410，例如一个摩托罗拉 PC 微处理器或者一个英特尔奔腾微

处理器。一个输入设备 420 例如一个键盘和鼠标、以及一个输出装置 430 例如一个 CRT 显示器，经由信号总线 440 被连接到 CPU410。一个通信接口 450、一个数据存储装置 460 例如 ROM 或者磁盘、以及一个 RAM470 经由信号总线也被连接到 CPU410。 如图 1 所示及描述的那样，通信接口 450 被连接到客户机 114 上。

操作系统 480，包括一个用于控制 CPU410 处理过程的程序，通常被存储在数据存储装置 460、并且被装入 RAM470 用于执行。操作系统 480 也包括一个通信引擎 482，用于产生信息数据包、并经由通信接口 450 与客户机 114 或全球服务器 106 交换信息数据包。操作系统 480 进一步包括用于商讨与用户的安全通道的安全服务 484、一个用于开放与用户之间的安全通道的通信引擎 486、以及一个用于为用户提供服务 110a-110d 的服务引擎 490。

服务引擎 490 包括一个服务接口 492，用于接收并翻译当前在客户机 114 执行的与下载的应用小程序 288 交换的信息，并且包括一个服务处理机 494 和服务数据 496 用于处理来自用户的服务请求。服务数据 496 可以包括先前产生的文件、数据库信息等等。 应该理解，服务数据 496 类似于用户数据 392，以至于包括相同的信息类型，但是它是在工作服务器 108 上被维护，不是在全球服务器 108 上。

图 5 是一个流程图，图示了使得用户能够在计算机网络系统 100 上访问服务 110a-110d 的方法 500。 该方法 500 由客户机 114 以步骤 505 开始，此步骤产生一个与全球服务器 106 的通信联络。参考图 6，步骤 505 将被更详细地描述。在步骤 510 中，全球服务器 106 确认用户有访问全球服务器 106 的功能的特权。确认用户访问特权的步骤可以包括检查用户证书、获得秘密口令、利用数字签名技术等等。应该理解，安全服务 384 可以使得小服务程序主机引擎 386 经由通信通道把安全应用小程序 389 传送到客户机 114，以用于执行用户认证。

在用户访问特权被确认之后，全球服务器 106 的网页引擎 387，在步骤 515 中把网页数据 391 和配置数据 390 下载到客户机 114。 在步骤 520 中，客户机 114 的浏览器 284 利用网页数据 391 和配置数据

390、在客户机 114 的输出装置上显示网页 700(图 7）并且使得它能够访问由全球服务器 106 提供的服务 110a-110d。一个示例性的网页 700 将如图 7 被显示和描述。

在步骤 525 中，经由输入设备 220，用户从列出的网页 700 选项中选择一项服务 110a-110d。作为响应，在步骤 530 中，全球服务器 106 的主机引擎 386 把相应的应用小程序(s)388、应用小程序配置数据 390、用户数据 392 以及可能的服务地址信息 394 下载到客户机 114。应用小程序配置数据 390，最好包括用户特定的参数选择例如用户偏爱的字体，用于配置选中的服务 110a-110d。用户数据 392 可以包括用户特定的以及服务特定的信息，例如存储的书签、日历数据、寻呼机编号等等。服务地址信息 394 识别选中的服务 110a-110d 的站点。也可以，相应的应用小程序 388、应用小程序配置数据 390、用户数据 392 以及服务地址信息 394，在步骤 515 中已经与网页数据 391 以及配置数据 390 一起被下载。

在步骤 535 中，客户机 114 的应用小程序引擎 286 执行相应的下载的应用小程序 288。工作服务器 108 在步骤 537 中初始化服务引擎 490。全球服务器 106 在步骤 538 中选择图 8A-8C 中所描述的三种访问模式之一，用于使得客户计算机 114 能够与相应的服务引擎 490 联络。例如，如果用户选择服务器 108c 上的服务 110d，它不被分离的防火墙保护，那么全球服务器 106 可能使用户能够直接访问。如果用户选择由公司网络 118 内的服务器 108a 提供的服务 110a，那么全球服务器 106 可以为用户提供直接的访问。应该理解，每一个防火墙 106 以及 120 可以存储策略，此种策略建立全球服务器 106 应该选择的访问的正确模式。其它选择访问模式的因素可以包括用户偏爱性、有效性以及可行性。在步骤 540 中，全球服务器 106 为客户机 114 提供到选中的服务 110a-110d 的访问。参考图 8A、8B 以及 8C，步骤 540 将更详细地描述。

图 6 是一个流程图，图示了步骤 505 的细节，此步骤从步骤 605 开始，在步骤 605 中用户通过客户机 114 利用已知的 URL 调用全球服

务器 106。在步骤 607 中，全球服务器 106 和客户机 114 之间建立一个安全通信通道，有可能是通过应用安全槽层(SSL)技术。即在步骤 610 中，全球服务器 106 的安全服务 384 确定联接安全通信是否许可，并且假如许可的话，建立一个与客户机 114 的通信通道。在步骤 615 中，客户机 114 的浏览器 284 和全球服务器 106 的安全服务 384，协商安全通信通道参数，有可能是利用公用密匙鉴定。一例安全通信通道是使用 RC4 加密的 RSA。应该理解全球服务器 106 可以被配置用来利用十种加密协议中的一种，并且客户机 114 可以被激活以利用五种加密协议中的一种。因此，步骤 615 可以包括选择一种对全球服务器 106 和客户机 114 通用的加密协议。在步骤 620 中，客户机 114 的加密引擎 285 和全球服务器的安全通信引擎 396，利用安全通道参数来建立安全通信通道。 之后，方法 505 也就结束了。

图 7 图示了一个示例性的基于 URL 可寻址超文本标记语言(HTML)的网页 700，此网页由小服务程序主机引擎 386 维护。网页 700 包括一个标题 710“网页”、提供的服务 715 的列表以及一个用于选择一种可供选择的服务 715 的指针 770。正如图示的那样，提供的服务 715 可以包括一个电子邮件服务 720、一个日历服务 730、一个互联网访问服务 740、一个页面调度服务 750 以及一部传真发送服务 760。虽然图中未示，网页 700 可以包括其它服务例如书签、快速查寻卡（QuickCard）等等。

图 8A 是一个流程图，图示了第一实施例中步骤 540 的细节，这里指的是步骤 540a，其中全球服务器 106 为客户机 114 提供到服务 110a-110d 的定向连接。步骤 540 由步骤 805 中下载的应用小程序 288 开始，从数据存储装置 360 中检索服务 110a-110d 的选中的服务地址、以及从密钥保存 395 检索用于服务 110a-110d 的认证信息。在步骤 810 中，通信引擎 282 在检索的服务地址处与工作服务器 108 的通信引擎 482 建立一个直接的、安全的连接，并且利用认证信息认证它本身。 在步骤 815 中，应用小程序 288 充当与服务引擎之间的输入/输出接口。然后步骤 540 就结束。

图 8B 是一个流程图，图示了第二实施例中步骤 540 的细节，这里指的是步骤 540b，其中全球服务器 106 作为客户机 114 到服务 110a-110d 的一个代理。步骤 540b 始于步骤 840，在步骤 840 中，应用小程序 288 检索服务地址，此地址导致步骤 540b 被指示到全球服务器 106。这样，在步骤 845 中,应用小程序 288 与全球服务器 106 之间建立了连接。在步骤 850 中，全球服务器 106 的小服务程序主机引擎 386，检索选中的服务 110a-110d 的服务地址、以及来自密钥保存 395 的用于此选中服务 110a-110d 的认证信息。在步骤 855 中，为创建一个与工作服务器 108 的安全通信引擎 486 之间的安全通道，全球服务器 106 的安全通信引擎 396 协商安全通道参数。

之后，在步骤 860 中,应用小程序 288 充当与全球服务器 106 的安全通信引擎 396 之间的输入/输出接口(使得用户能够作出服务引擎 490 的请求)。在步骤 865 中，如果小服务程序主机引擎 386 确定执行客户机 114 用户的请求是未经认证的话，那么小服务程序主机引擎 386 在步骤 870 中就会确定是否方法 540b 已经结束，例如用户是否已经退出。假如是的话，那么方法 820b 就会结束。否则，方法 540b 返回到步骤 860 以获得另一个请求。在步骤 865 中，如果小服务程序主机引擎 386 确定执行客户机 114 用户的请求是经过认证的话，小服务程序主机引擎 386，就可能利用小服务程序 398 充当客户机 114 到服务引擎 490 的代理。作为代理，小服务程序主机引擎 386 为应用小程序 288 把服务请求传送到服务 110a-110d，并且把回应传送到当前执行在客户机 114 上正在请求的应用小程序 288。方法 540b 接着返回步骤 870。

图 8C 是一个流程图，图示了第三个实施例中步骤 540 的细节，这里指的是步骤 540c，其中被请求的服务 110a-110d 位于全球服务器 106。步骤 540e 始于步骤 880，在步骤 880 中，应用小程序 288 为服务 110a-110d 检索服务地址，这样就会为应用小程序 288 提供全球服务器 106 上的服务 110a-110d 的服务地址。这样，在步骤 882 中应用小程序 288 与全球服务器 106 之间建立了一个连接。因为在图 5 所示的步骤 510 中、客户机 114 已经把它本身识别并认证到全球服务器 106

上，就不再需要附加的识别步骤。

在步骤 884，判断服务 110a-110d 是否在当前运转。假如这样的话，那么在步骤 886 中就会判断服务 110a-110d 是否能够处理多个用户。如果不是，那么在步骤 890 中全球服务器 106 会为用户建立一个实例（instance），并且在步骤 532 中应用小程序 288 充当与全球服务器 106 上的服务 110a-110d 之间的输入/输出接口。否则，在步骤 886 中，如果服务 110a-110d 确定不能处理多个用户，那么方法 540a 就会进入步骤 892。进一步，在步骤 884 中，如果全球服务器 106 确定当前服务 110a-110d 没有执行，那么全球服务器 106 在步骤 888 中就会起动服务 110a-110d，并且进入到步骤 886。

上文所述本发明最佳实施例的描述，仅仅是为了举例，并且上述实施例的其它变化和方法也可由本发明提供。 本发明的部件可以通过下面的方法实现，利用可编程的通用数字计算机、利用应用程序特定的集成电路、或者利用互相连接的常规部件和电路的网络。在此已经描述了用于说明的实施例，但并不限制于此。 按照上文的教导，可以产生许多变化、作出许多改进。本发明仅由下面的权利要求限制。

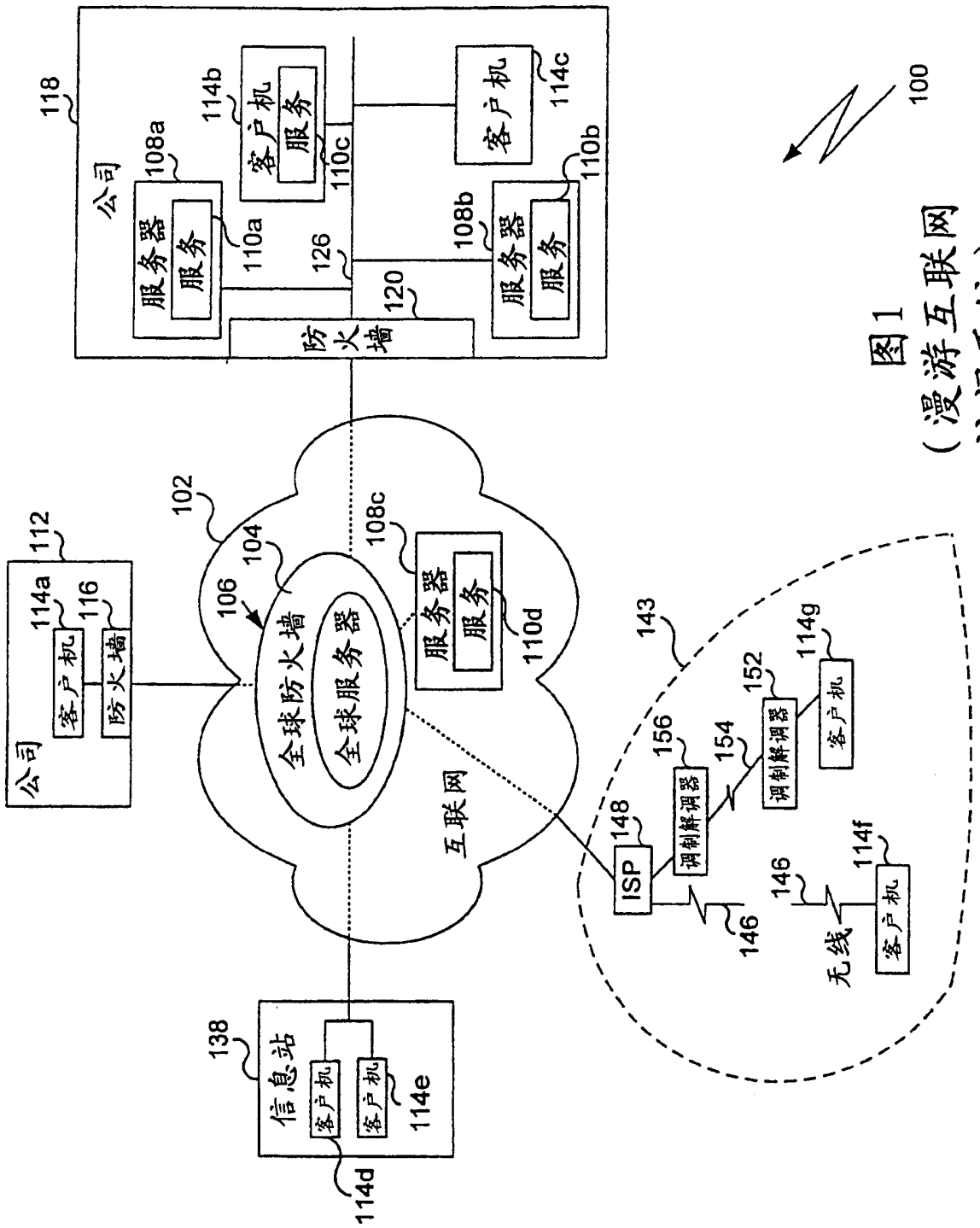


图1
（漫游互联网访问系统）

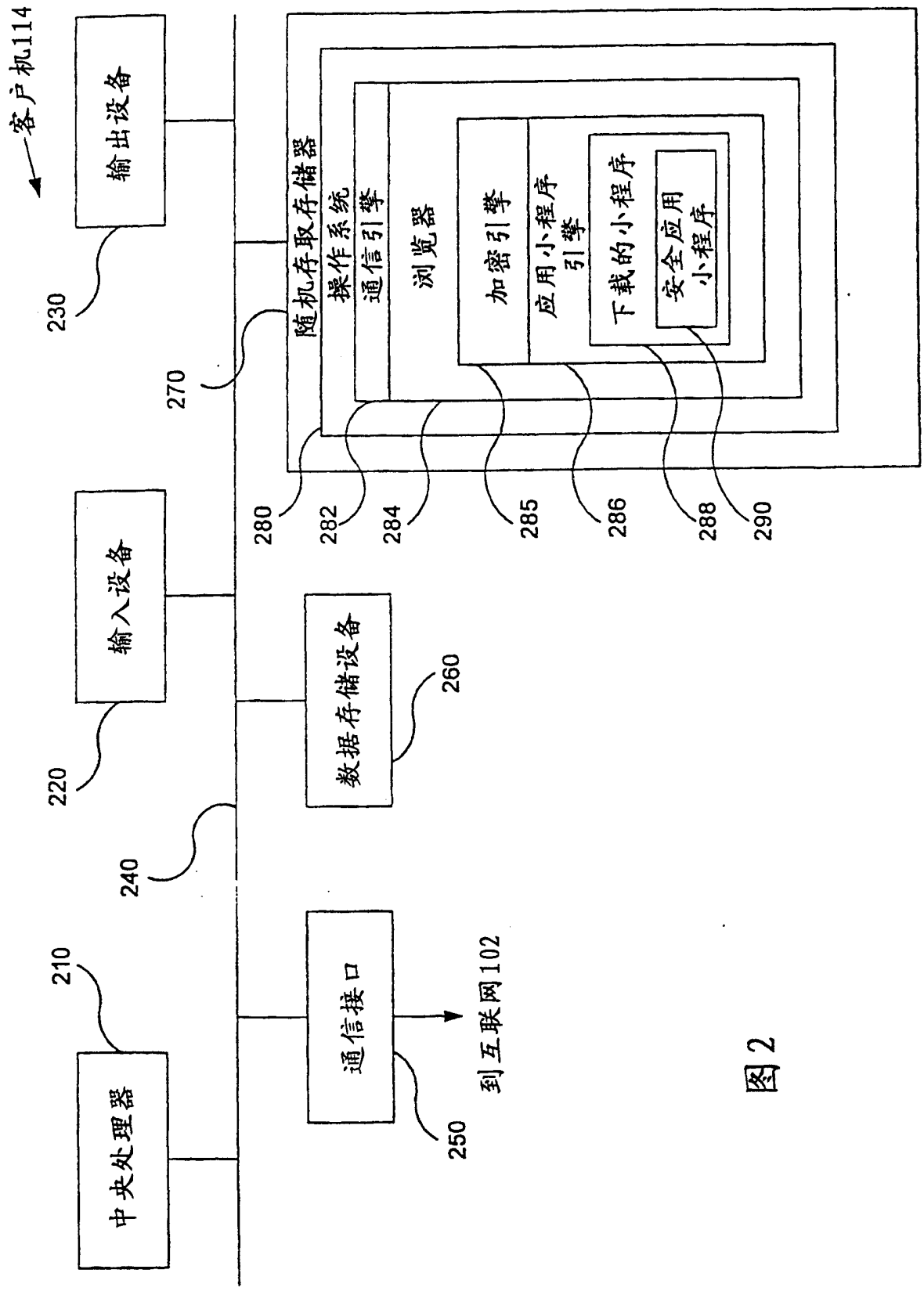

客户机114
输出设备
230
270
随机存取存储器
操作系统
通信引擎
浏览器
加密引擎
应用小程序引擎
下载的小程序
安全应用小程序
280
282
284
285
286
288
290
输入设备
220
数据存储设备
260
240
210
通信接口
到互联网102
250
中央处理器

图 2

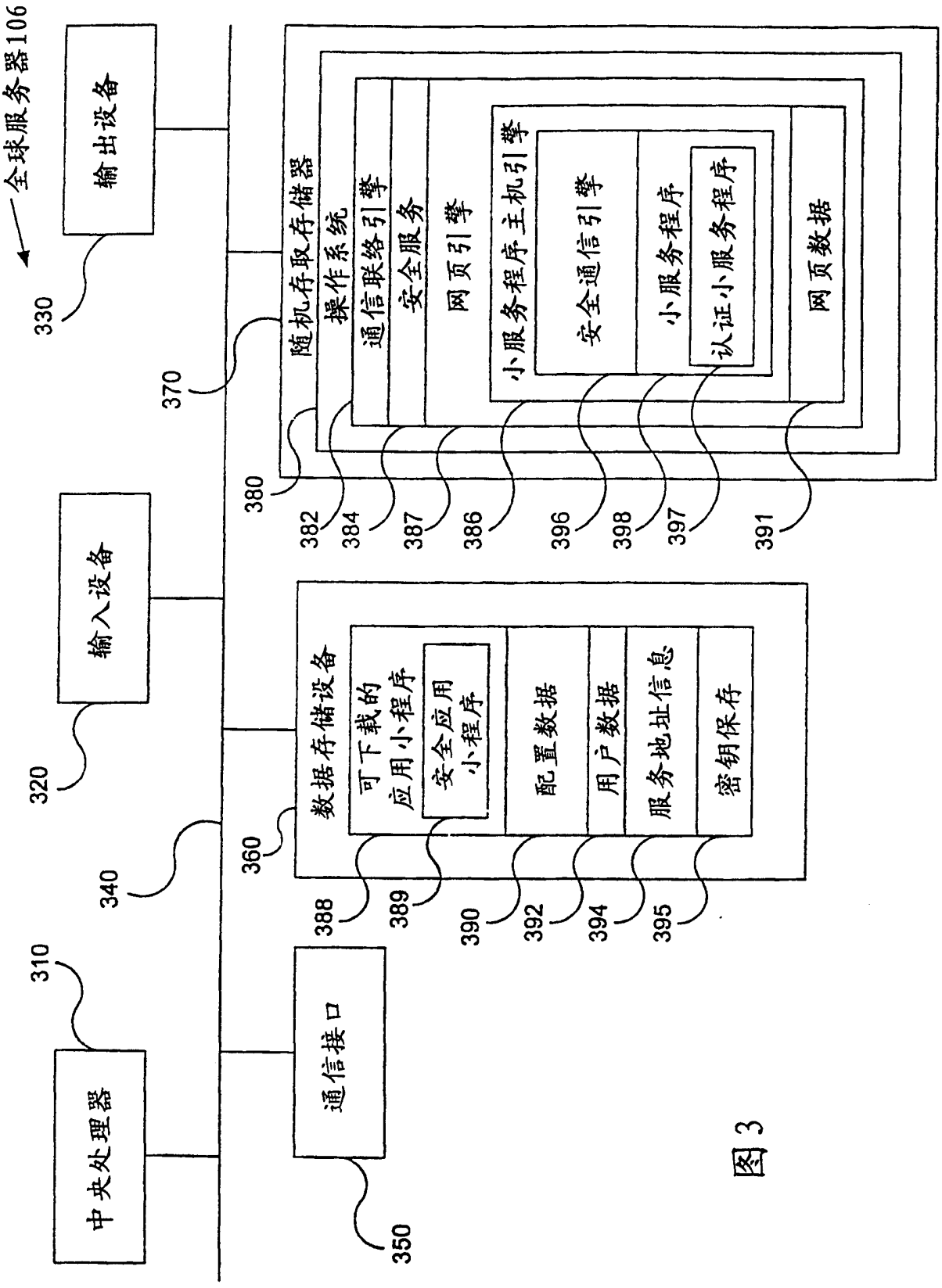

全球服务器106
输出设备
330
370
随机存取存储器
操作系统
通信联络引擎
安全服务
网页引擎
小服务程序主机引擎
安全通信引擎
小服务程序
认证小服务程序
网页数据
380
382
384
387
386
396
398
397
391
输入设备
320
340
数据存储设备
可下载的应用小程序
安全应用小程序
配置数据
用户数据
服务地址信息
密钥保存
360
388
389
390
392
394
395
310
中央处理器
通信接口
350

图 3

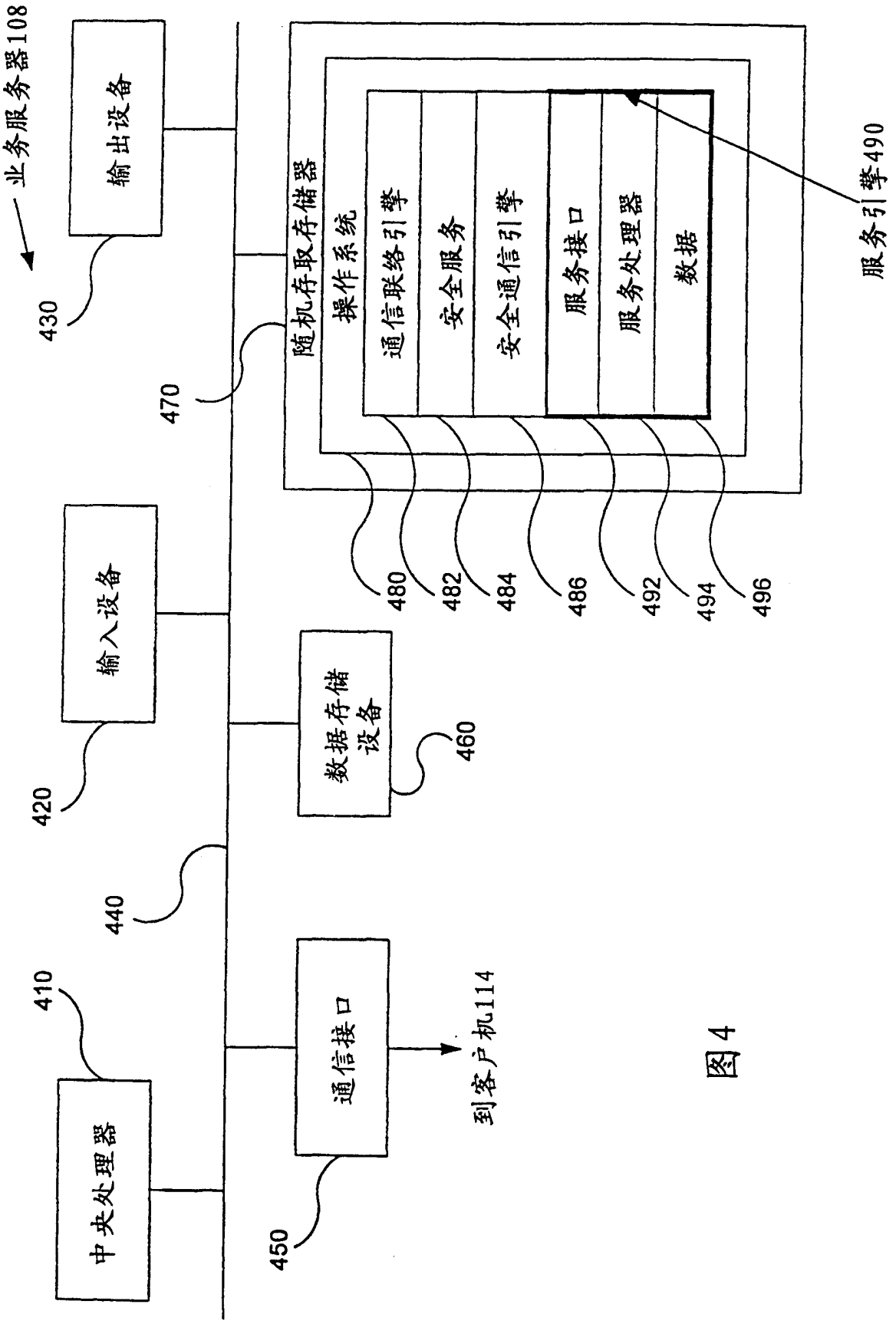

业务服务器108
输出设备
430
随机存取存储器
操作系统
通信联络引擎
安全服务
安全通信引擎
服务接口
服务处理器
数据
服务引擎490
470
480
482
484
486
492
494
496
输入设备
420
数据存储设备
460
440
410
中央处理器
通信接口
450
到客户机114

图 4

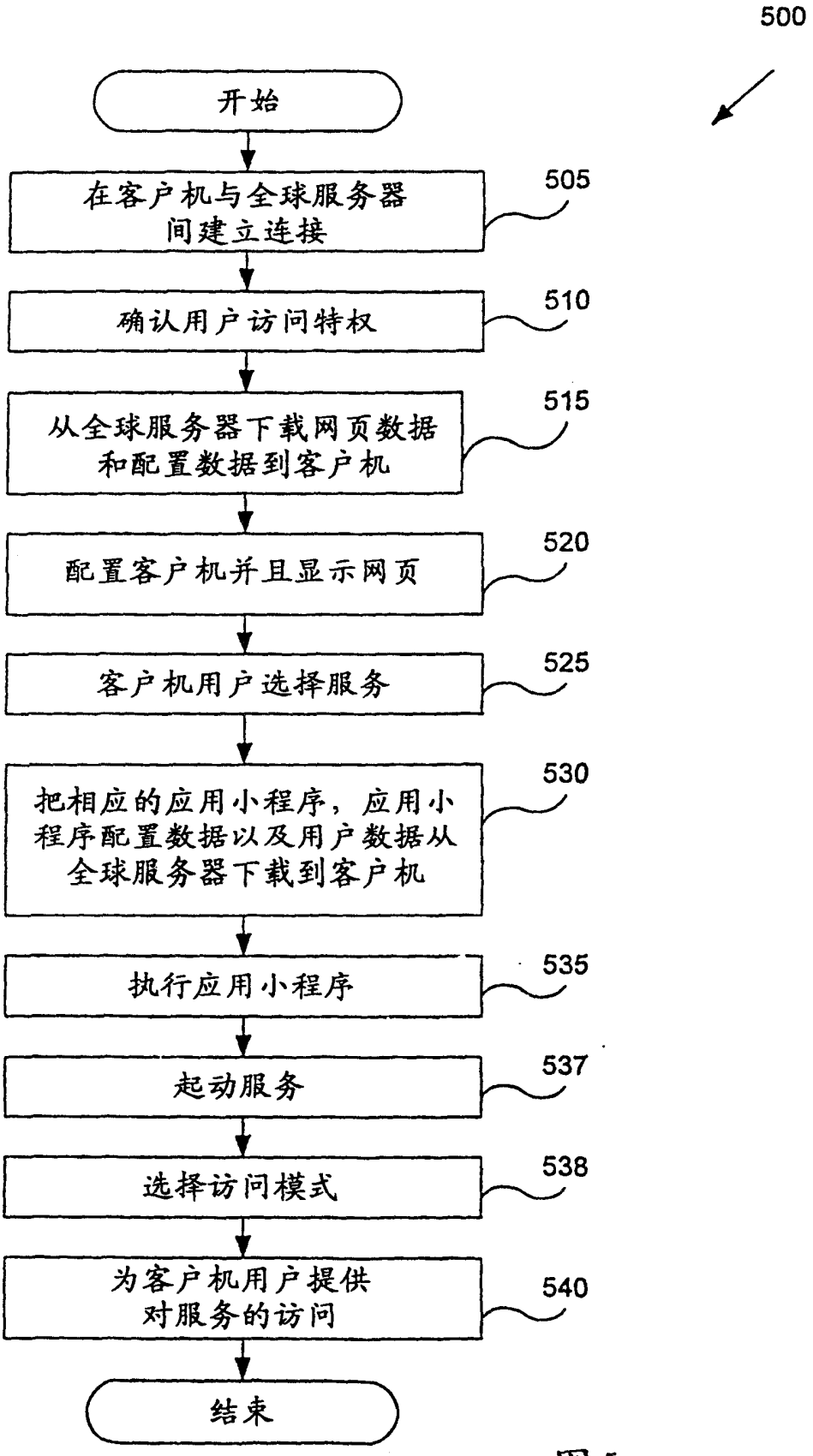

500
开始
在客户机与全球服务器间建立连接
505
确认用户访问特权
510
从全球服务器下载网页数据和配置数据到客户机
515
配置客户机并且显示网页
520
客户机用户选择服务
525
把相应的应用小程序，应用小程序配置数据以及用户数据从全球服务器下载到客户机
530
执行应用小程序
535
起动服务
537
选择访问模式
538
为客户机用户提供对服务的访问
540
结束

图5

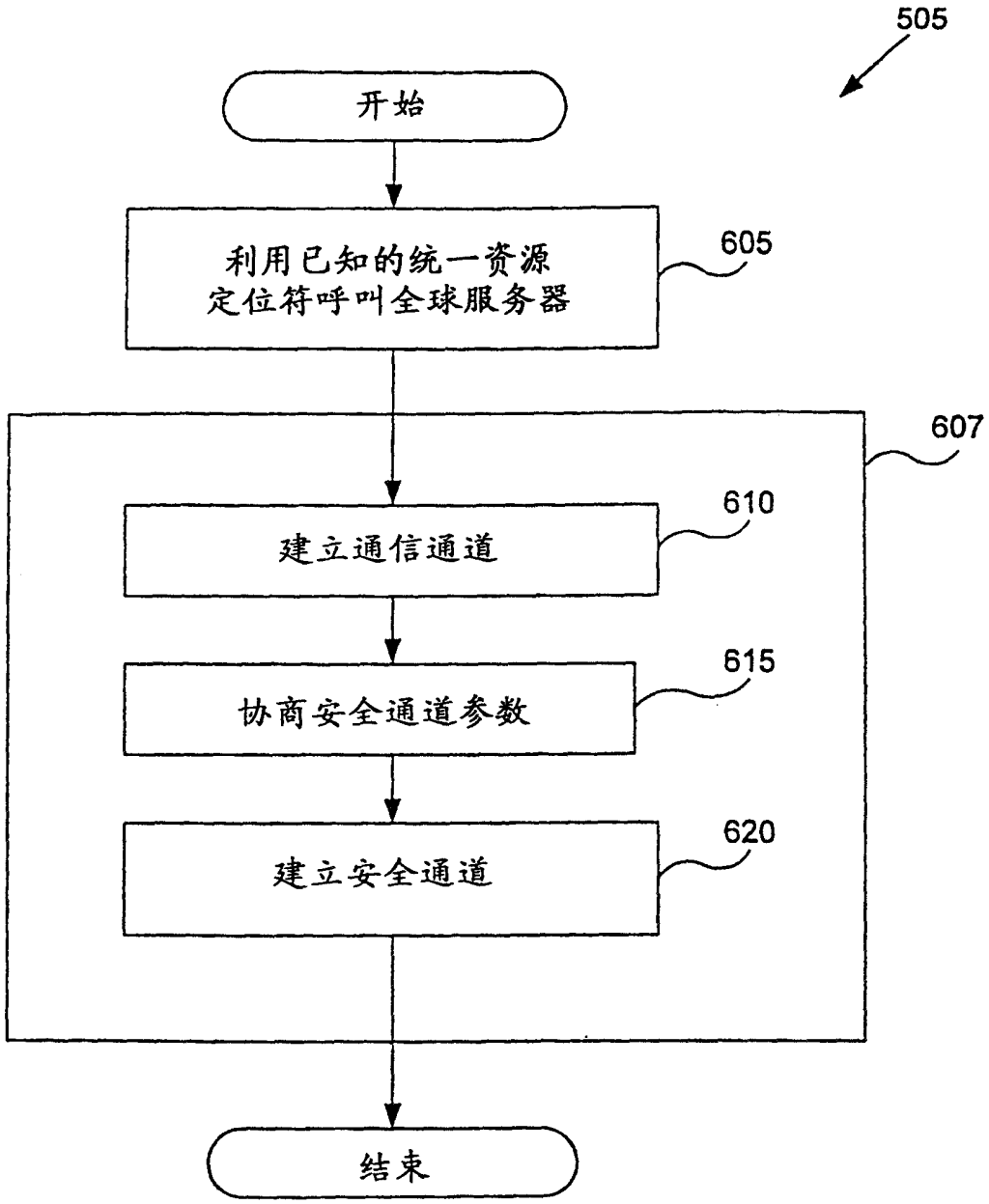

505
开始
利用已知的统一资源
定位符呼叫全球服务器
605
607
610
建立通信通道
615
协商安全通道参数
620
建立安全通道
结束

图6

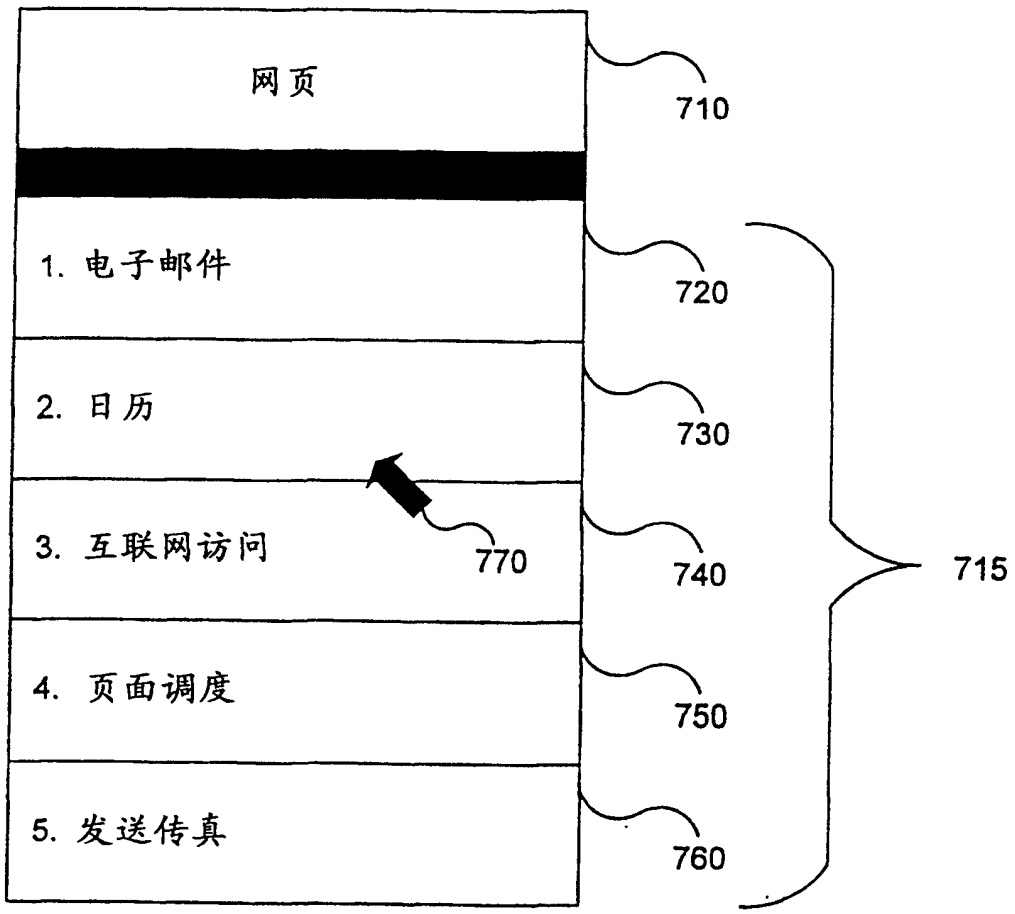

网页
710
1. 电子邮件
720
2. 日历
730
3. 互联网访问
770
740
715
4. 页面调度
750
5. 发送传真
760

图7
（页面屏幕显示）

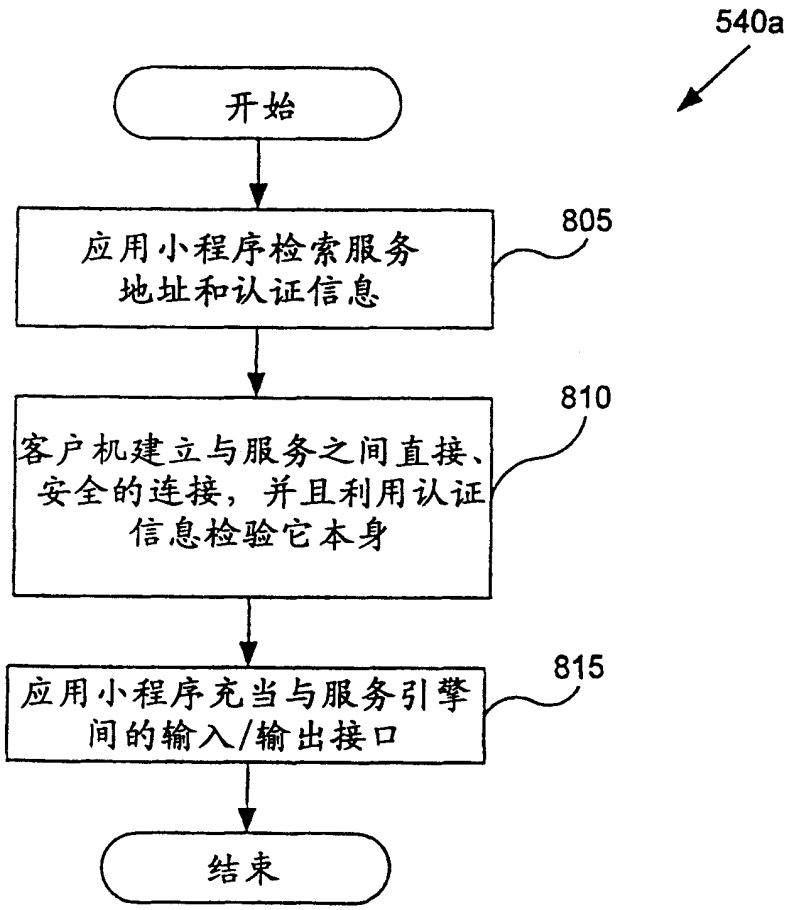

540a
开始
应用小程序检索服务地址和认证信息
805
客户机建立与服务之间直接、安全的连接，并且利用认证信息检验它本身
810
应用小程序充当与服务引擎间的输入/输出接口
815
结束

图8A
（重定位）

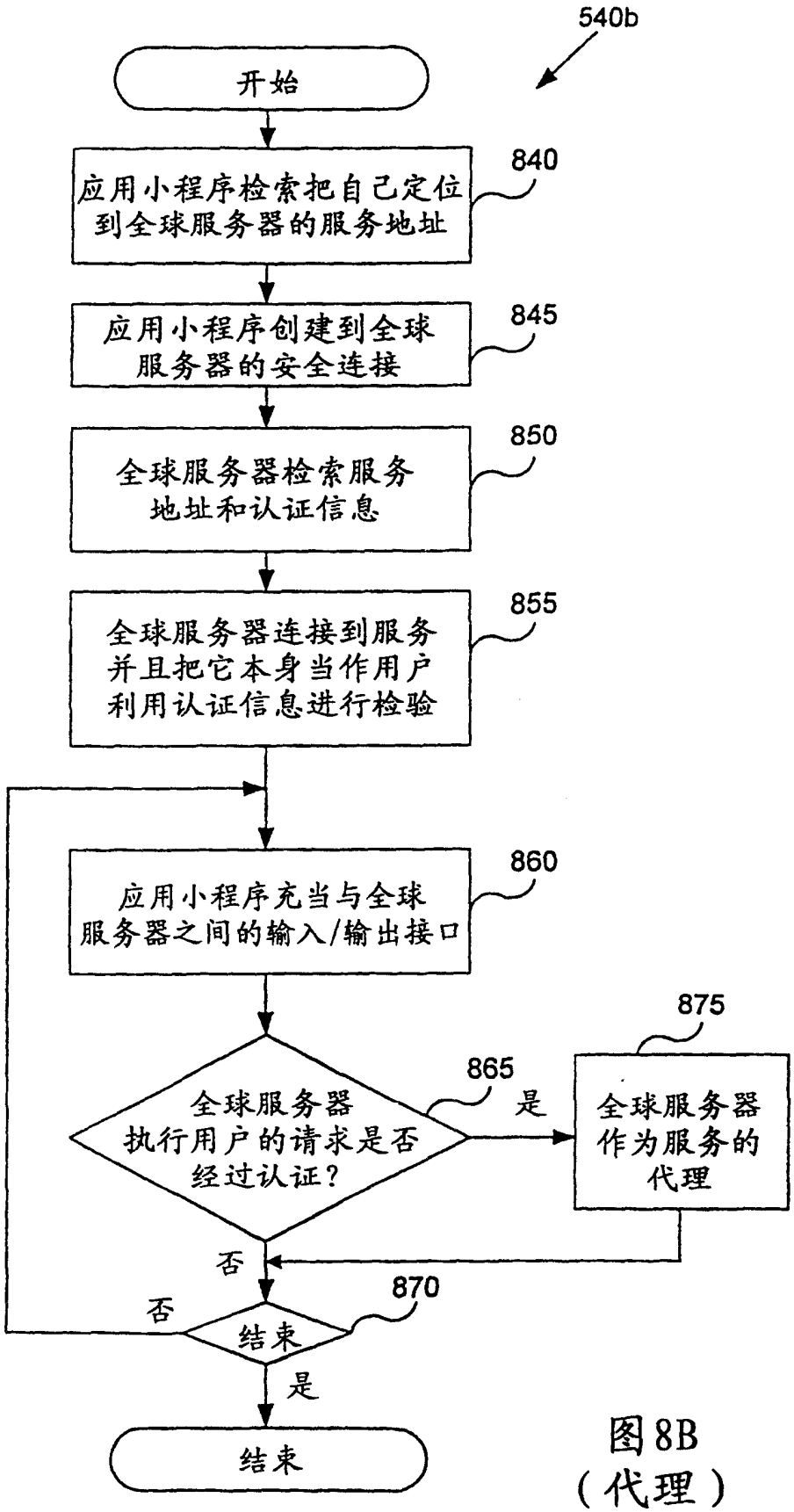

540b
开始
应用小程序检索把自己定位到全球服务器的服务地址
840
应用小程序创建到全球服务器的安全连接
845
全球服务器检索服务地址和认证信息
850
全球服务器连接到服务并且把它本身当作用户利用认证信息进行检验
855
应用小程序充当与全球服务器之间的输入/输出接口
860
全球服务器执行用户的请求是否经过认证?
865
是
全球服务器作为服务的代理
875
否
结束
870
否
是
结束

图8B
（代理）

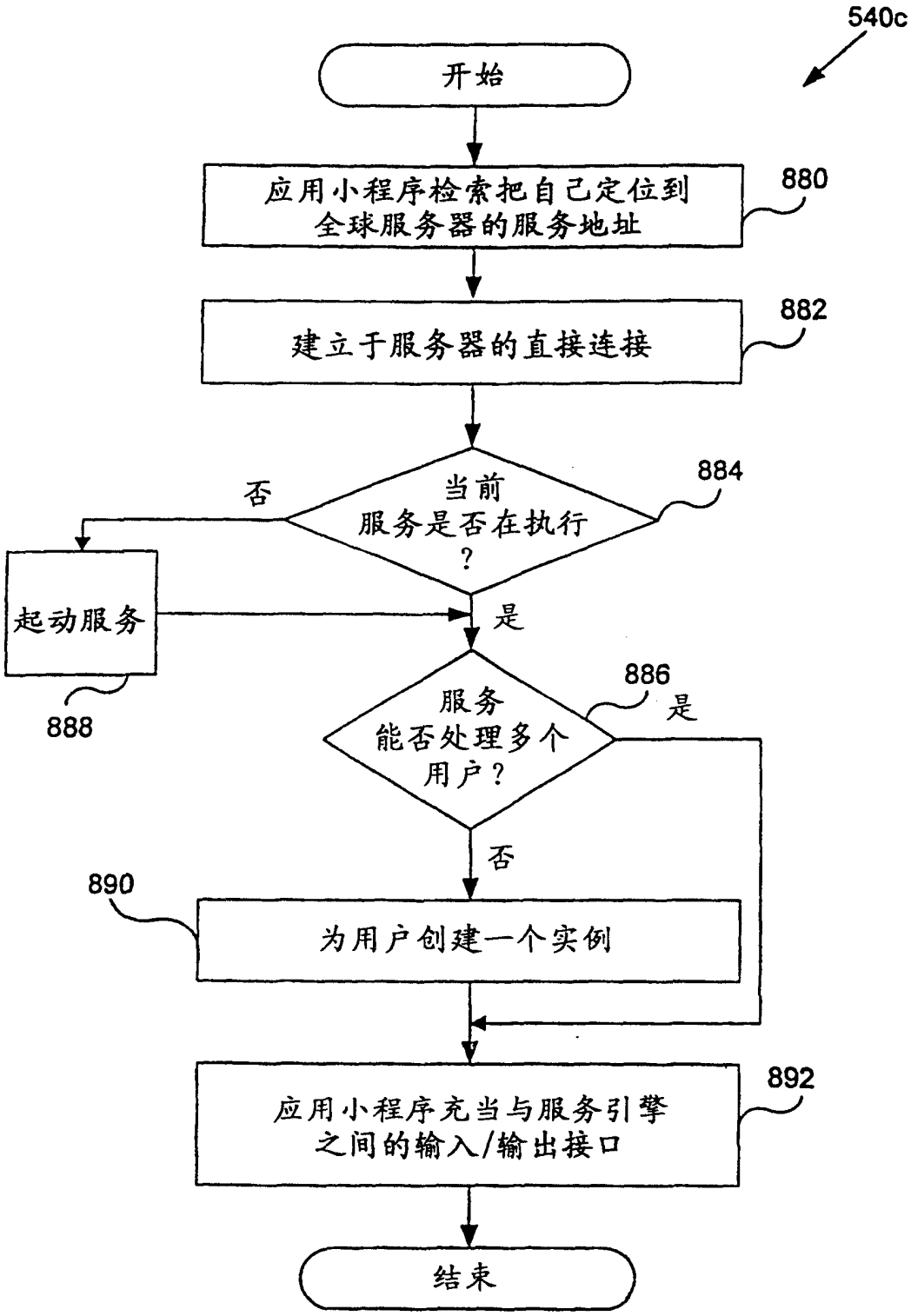

540c
开始
应用小程序检索把自己定位到全球服务器的服务地址
880
建立于服务器的直接连接
882
当前服务是否在执行？
884
否
起动服务
888
是
服务能否处理多个用户？
886
是
否
890
为用户创建一个实例
应用小程序充当与服务引擎之间的输入/输出接口
892
结束

图8C
（定位到数据）