[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 9/00 (2006.01)

[12] 发明专利申请公布说明书

[21] 申请号 200780043423.X

[43] 公开日 2009 年 12 月 23 日

[11] 公开号 CN 101611588A

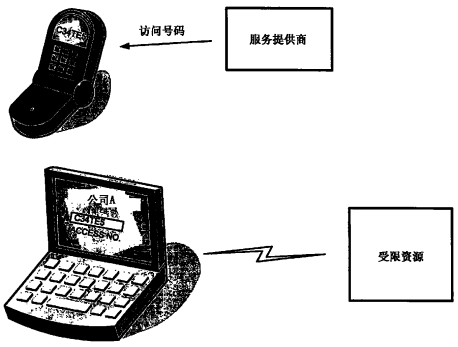
[22] 申请日 2007.11.20
[21] 申请号 200780043423.X
[30] 优先权
[32] 2006.11.22 [33] US [31] 11/562,607
[86] 国际申请 PCT/US2007/085206 2007.11.20
[87] 国际公布 WO2008/127430 英 2008.10.23
[85] 进入国家阶段日期 2009.5.22
[71] 申请人 威瑞森全球商务有限责任公司
地址 美国新泽西州
[72] 发明人 亚历山大·菲诺格诺夫
[74] 专利代理机构 中原信达知识产权代理有限责任公司
代理人 张焕生 安 翔
权利要求书 5 页 说明书 11 页 附图 8 页

[54] 发明名称

对于受限资源的安全访问

[57] 摘要

一种系统可以生成访问号码，将该访问号码经由电话呼叫提供给用户，并且将该访问号码提供给认证服务器。 该系统可以基于提供给用户的访问号码和提供给认证服务器的访问号码来管理用户对受限资源的访问。



1. 一种方法包括：

从用户接收电话呼叫；

认证所述用户；

当所述用户被认证时，生成访问号码；以及

将所述访问号码发送至所述用户和认证服务器，以便基于发送至所述用户的所述访问号码和发送至所述认证服务器的所述访问号码来管理对受限资源的访问。

2. 根据权利要求1所述的方法，其中，所述用户使用电话设备进行所述电话呼叫；以及

其中，认证所述用户包括：

确定与所述电话设备相关联的第一识别信息，

确定与所述用户相关联的第二识别信息，以及

基于所述第一识别信息和所述第二识别信息，认证所述用户。

3. 根据权利要求2所述的方法，其中，确定与所述电话设备相关联的第一识别信息包括：

确定呼叫方识别（ID）信息或国际移动用户身份信息中的至少一个。

4. 根据权利要求2所述的方法，其中，确定与所述用户相关联的第二识别信息包括：

从所述用户接收密码或生物量测数据中的至少一个。

5. 根据权利要求2所述的方法，其中，生成访问号码包括：

生成随机字符串，以及

将所述第一识别信息或所述第二识别信息中的一个嵌入所述随机字符串中，作为所述访问号码。

6. 根据权利要求1所述的方法，进一步包括：

当所述用户未被认证时，在没有将所述访问号码发送至所述用户的情况下，使所述电话呼叫断开连接。

7. 根据权利要求1所述的方法，其中，生成所述访问号码包括：

生成预定长度的随机字符串作为所述访问号码。

8. 根据权利要求1所述的方法，其中，生成所述访问号码包括：

生成具有指示所述访问号码何时到期的到期时间的预定长度的随机字符串作为所述访问号码。

9. 根据权利要求1所述的方法，进一步包括：

确定所述用户与多个公司相关联，所述公司中的每个包括相应的认证服务器；以及

其中，发送所述访问号码包括：

将所述访问号码传送至与所述多个公司相对应的所述认证服务器。

10. 一种系统，包括：

服务提供商，用于：

从用户接收电话呼叫；

认证所述用户；

当所述用户被认证时，生成访问号码；以及

将所述访问号码提供给所述用户作为第一访问号码，并且提供给认证服务器作为第二访问号码，以便基于所述第一访问号码和所述第二访问号码来管理对受限资源的访问。

11. 根据权利要求10所述的系统，其中，所述用户使用电话设备进行所述电话呼叫；以及

其中，当认证所述用户时，所述服务提供商服务器被配置成：

确定与所述电话设备相关联的第一识别信息，

确定与所述用户相关联的第二识别信息，以及

基于所述第一识别信息和所述第二识别信息，认证所述用户。

12. 根据权利要求11所述的系统，其中，所述第一识别信息包括呼叫方识别（ID）信息或国际移动用户身份信息中的至少一个。

13. 根据权利要求11 所述的系统，其中，所述第二识别信息包括与所述用户相关联的密码或生物量测数据中的至少一个。

14. 根据权利要求11所述的系统，其中，当生成所述访问号码时，所述服务提供商被配置成：

生成随机字符串，以及

将所述第一识别信息或所述第二识别信息中的一个嵌入所述随机字符串中，作为所述访问号码。

15. 根据权利要求10所述的系统，其中，所述访问号码包括具有指示所述访问号码何时到期的到期时间的预定长度的随机字符串。

16. 根据权利要求10所述的系统，其中，所述认证服务器被配置成：

从所述用户接收所述第一访问号码，

确定所述第一访问号码是否有效，

将所述第一访问号码和所述第二访问号码相比较，以及

当所述第一访问号码有效并且所述第一访问号码与所述第二访问号码匹配时，确定所述用户被允许访问所述受限资源。

17. 根据权利要求16所述的系统，其中，所述访问号码具有指示所述访问号码何时到期的到期时间；以及

其中，当确定所述第一访问号码是否有效时，所述认证服务器被配置成当所述第一访问号码尚未到期时，确定所述第一访问号码有效。

18. 一种系统，包括：

认证服务器，用于：

从服务提供商接收第一访问号码；

从用户接收第二访问号码，所述第二访问号码经由电话呼叫从所述服务提供商被提供给所述用户；

确定所述第二访问号码是否有效；

将所述第一访问号码和所述第二访问号码相比较；以及

基于所述第二访问号码是否有效以及所述第一访问号码和所述第二访问号码的所述比较的结果，向所述用户提供对受限资源的选择性访问权。

19. 根据权利要求18所述的系统，其中，所述第二访问号码具有指示所述第二访问号码何时到期的到期时间；以及

其中，当确定所述第二访问号码是否有效时，所述认证服务器被配置成当所述第二访问号码尚未到期时，确定所述第二访问号码有效。

20. 根据权利要求18所述的系统，其中，当提供对所述受限资源的选择性访问权时，所述认证服务器被配置成当所述第二访问号码有效并且所述第一访问号码匹配所述第二访问号码时，确定所述用户被允许访问所述受限资源。

21. 根据权利要求18所述的系统，其中，所述认证服务器进一步被配置成在基于所述第二访问号码提供了对所述受限资源的选择性访问权之后，使所述第二访问号码到期。

22. 根据权利要求18所述的系统，其中，当提供对所述受限资源的选择性访问权时，所述认证服务器被配置成当所述用户被允许访问

所述受限资源时，将消息发送至所述受限资源或管理对所述受限资源的访问的设备，所述受限资源或设备授予所述用户对所述受限资源的访问权。

23. 一种系统，包括：

用于生成访问号码的装置；

用于经由电话呼叫将所述访问号码提供至用户的装置；

用于将所述访问号码提供至认证服务器的装置；以及

用于基于提供给所述用户的所述访问号码以及提供给所述认证服务器的所述访问号码来管理所述用户对受限资源的访问的装置。

对于受限资源的安全访问

背景技术

许多公司使用诸如令牌设备的安全设备，以管理对它们的受限资源的访问。公司将令牌设备发给其雇员和/或客户。令牌设备生成随时间（例如，每1分钟）改变的号码。公司的服务器也生成跟踪由这些令牌设备生成的号码的号码。由公司的服务器生成的号码在时间上与由令牌设备生成的号码同步。

当用户试图获得对该公司的受限资源的访问权时，用户将在其令牌设备上当前所示的号码提供给公司的服务器，并且提供个人识别号码（PIN）。该公司的服务器基于用户提供的号码与它所生成的号码匹配以及用户的PIN来管理对受限资源的访问。

令牌设备是昂贵的。虽然每个令牌设备本身可能不太昂贵，但是当为公司所有雇员和/或客户购买令牌设备时，它就变得昂贵了。而且，令牌设备需要周期性地更换（例如，每三年）。因此，令牌设备成为持续性的开支。而且，如果雇员/客户丢失或忘记了其令牌设备，则雇员/客户就无法访问该公司的受限资源。

附图说明

图1是图示此处所描述的概念的示例性视图；

图2是其中可以实现此处所描述的系统和方法的网络的示例性视图；

图3是可以与图2的电话设备、服务提供商服务器、计算机设备和/或认证服务器中的一个或多个相对应的设备的示例性视图；

图4是用于选择性地提供对受限资源的访问权的示例性过程的流程图；

图5A-5B是图示图4的过程的部分的电话设备的示例性视图；

图6是图示图4的过程的部分的计算机设备的示例性视图；

图7是其中可以实现此处所描述的系统和方法的另一网络的示例性视图；以及

图8是其中可以实现此处所描述的系统和方法的又一网络的示例性视图。

具体实施方式

下列具体描述参考了附图。在不同附图中相同的附图标记可以表示相同或类似的元件。而且，下列详细描述并不限制本发明。

此处所描述的实施方式可以便于对受限资源的选择性访问。图 1 是图示此处所描述的概念的示例性视图。如图 1 所示，用户可以使用蜂窝电话来联系服务提供商。用户可以使用例如识别该用户的蜂窝电话（例如，呼叫方识别（ID））的信息以及可能的密码（例如，任何字母、数字和/或符号的组合）向服务提供商认证自身。如果用户被适当地认证，则服务提供商可以提供可以在蜂窝电话的显示器上显示的访问号码。用户可以将该访问号码输入提供对受限资源的访问权的计算机设备的用户界面中。该访问号码可以用于认证该用户，并且提供对受限资源的选择性访问权。

图 2 是其中可以实现此处所描述的系统和方法的网络 200 的示例性视图。网络 200 可以包括经由网络 230 连接至服务提供商服务器 220 的电话设备 210，以及经由网络 270 连接至认证服务器 250 和受限资源 260 的计算机设备 240。出于简明目的，单个电话设备 210、服务提供商服务器 220、计算机设备 240、认证服务器 250 以及受限资源 260 已经被图示为连接至网络 230 和 270。在实践中，可以存在更多或更少的电话设备、服务提供商服务器、计算机设备、认证服务器和/或受限资源。

而且，在单个设备中实现电话设备210、服务提供商服务器220、计算机设备240、认证服务器250和/或受限资源260的某种组合是可能的。例如，电话设备210和计算机设备240可以被实现为单个设备，认证服务器250和受限资源260可以被实现为单个设备，和/或计算机设备240和受限资源260可以被实现为单个设备。

电话设备210可以包括任何类型或形式的通信设备，诸如蜂窝电话、无绳电话、有线电话、卫星电话、无线电话、智能电话等。用户可以使用电话设备210来联系服务提供商服务器220。

服务提供商服务器220可以包括能够经由网络230和网络270通信的设备，诸如计算机系统。在一个实施例中，服务提供商服务器220可以被实现为单个设备。在另一实施例中，服务提供商服务器220可以被实现为位于同地或相互远离的多个设备。

计算机设备240可以包括任何类型或形式的计算或通信设备，诸如个人计算机、膝上型计算机、个人数字助理（PDA）等。计算机设备240的用户可以试图经由认证服务器250获得对受限资源260的访问权。认证服务器250可以包括能够关于受限资源260的选择性访问而认证用户的设备，诸如计算机系统。在一个实施例中，认证服务器250可以基于来自服务提供商服务器220的访问号码来允许对受限资源260的访问。受限资源260可以包括可以控制对其的访问的任何类型或形式的资源，诸如专用网络（例如，公司内部网络）、设备（例如，计算机、存储设备或外围设备）、数据（例如，与用户的账户或简档相关联的数据）或软件（例如，电子邮件应用、文字处理程序或操作系统）。

网络230可以包括电话网络（诸如蜂窝网络、公共交换电话网络（PSTN））或网络的组合。网络270可以包括局域网（LAN）、广域网（WAN）、诸如PSTN或蜂窝网络的电话网络、内部网络、因特网

或网络的组合。网络 230 和网络 270 被实现为相同网络是可能的。

图 3 是可以与电话设备 210、服务提供商服务器 220、计算机设备 240 和/或认证服务器 250 中的一个或多个相对应的设备。该设备可以包括总线 310、处理器 320、主存储器 330、只读存储器（ROM）340、存储设备 350、输入设备 360、输出设备 370 以及通信接口 380。总线 310 可以包括允许在该设备的元件之间通信的路径。

处理器 320 可以包括处理器、微处理器或可以解释和执行指令的处理逻辑。主存储器 330 可以包括随机访问存储器（RAM）或可以存储供处理器 320 执行的信息和指令的另一类型的动态存储设备。ROM 340 可以包括 ROM 设备或可以存储供处理器 320 使用的静态信息和指令的另一类型的静态存储设备。存储设备 350 可以包括磁和/光记录介质及其相应的驱动器。

输入设备 360 可以包括允许操作员将信息输入该设备的机构，诸如键盘、鼠标、笔、语音识别和/或生物量测机制等。输出设备 370 可以包括将信息输出给操作员的机制，包括显示器、打印机、扬声器等。通信接口 380 可以包括任何类似收发器的机制，该机构使得该设备能够与其他设备和/或系统通信。例如，通信接口 380 可以包括用于经由诸如网络 230 或 270 的网络与另一设备或系统通信的机制。

如以下将详细描述的，图 3 所示的设备，如此处所描述的，可以执行与获取对受限资源 260 的选择性访问权相关的某些操作。该设备可以响应于处理器 320 执行在诸如存储器 330 的计算机可读介质中包含的软件指令来执行这些操作。计算机可读介质可以被定义为物理或逻辑存储设备和/或载波。

软件指令可以从诸如数据存储设备 350 的另一计算机可读介质或经由通信接口 380 从另一设备读入存储器 330 中。在存储器 330 中包

含的软件指令可以使得处理器320执行将在下文描述的过程。替代地，硬线电路可以取代软件指令或结合软件指令来使用，以实现此处所描述的过程。因此，此处所描述的实施方式不限于硬件电路和软件的任何特定组合。

图 4 是用于选择性地提供对受限资源的访问权的示例性过程的流程图。在一种实施方式中，图 4 的过程可以由在电话设备 210、服务提供商处理器 220、计算机设备 240、认证服务器 250 或电话设备 210、服务提供商处理器 220、计算机设备 240 和认证服务器 250 的组合中的一个或多个软件和/或硬件组件来执行。图 5A-5B 是图示图 4 的过程的部分的电话设备的示例性视图。图 6 是图示图 4 的过程的部分的计算机设备的示例性视图。

处理可以从发起对预定电话号码的电话呼叫开始（框 410）。例如，如图 5A 所示，用户可以将与服务提供商服务器 220 相关联的电话号码输入电话设备 210 中。当由用户指示时，电话设备 210 可以呼叫服务提供商服务器 220。

电话呼叫可以被接收，并且用户可以被认证（框 420 和 430）。例如，基于与电话设备 210 相关联的独特（unique）电话识别信息，诸如呼叫方 ID 信息，国际移动用户身份（IMSI）信息或对于电话设备 210 独特的其他信息，服务提供商服务器 220 可以识别该用户。基于特定于该用户的用户识别信息，诸如密码或生物量测数据（例如，语音信号），服务提供商服务器 220 可以识别电话设备 210 的用户。例如，服务提供商服务器 220 可以要求该用户提供用户识别信息，并且可以将该用户识别信息与先前与电话设备 210 相关联的识别信息相比较。多个用户与相同电话设备 210 相关联是可能的。在该情形下，服务提供商服务器 220 可以使用由用户提供的用户识别信息来确定该用户是否是这些用户中的一个，以及如果是，则是哪一个。

如果用户未被适当地认证，那么该呼叫可以被断开连接。然而，如果用户被适当地认证，则可以将访问号码提供给电话设备 210 和认证服务器 250（框 440）。例如，服务提供商服务器 220 可以包括硬件或软件访问号码生成器，该生成器被配置成生成预定长度的随机字符串（例如，数字、字母和/或符号的任何组合）以用作访问号码。在一种实施方式中，该访问号码可以包括嵌入其中的用户识别信息（或可能是电话识别信息）。在该情形下，可以生成随机字符串，并且然后，该字符串可以被修改以嵌入用户识别信息。用户识别信息可以以认证服务器 250 已知的方式嵌入，以便认证服务器 250 能够根据访问号码确定用户识别信息。

以不可再现的不可预测的方式生成访问号码是有益的（例如，通过黑客方式）。该访问号码可以具有某个到期时间（例如，1 分钟、5 分钟、30 分钟等），该到期时间指示该访问号码何时到期。为了安全目的，较短的到期时间与较长的到期时间相比更为有利。而且，该访问号码可以被设计成一次性使用，以便该访问号码可以一旦使用立即到期。

服务提供商服务器 220 可以将访问号码发送至电话设备 210。在一种实施方式中，如图 5B 所示，服务提供商服务器 220 可以在用于在电话设备 210 的显示器上呈现的消息中发送访问号码。服务提供商服务器 220 也可以将相同的访问号码发送至认证服务器 250。在一种实施方式中，服务提供商服务器 220 可以在消息中将访问号码连同关于用户的信息一起发送至认证服务器 250。认证服务器 250 可以使用该用户信息，以将随后的用户访问尝试与从服务提供商服务器 220 接收到的消息（以及因此，访问号码）相匹配。

在某个点，认证服务器 250 可以被联系（框 450）。例如，如图 6 所示，用户可以访问与计算机设备 240 或认证服务器 250 相关联的用户界面。在一种实施方式中，用户可以使用例如在计算机设备 240 上

设置的网络浏览器来访问用户界面。在另一实施方式中，在启动计算机设备 240 之后，可以自动向用户呈现用户界面。

可以将访问号码呈现到认证服务器 250（框 460）。例如，认证服务器 250 可以请求各种信息，以适当地认证该用户。在一种实施方式中，如图 6 所示，认证服务器 250 可以基于用户的用户名（例如，Billy West）以及访问号码（例如，46A9B39P）来认证该用户。如果访问号码包括嵌入其中的用户识别信息（或电话识别信息），则认证服务器 250 可以基于用户名、访问号码以及用户识别信息来认证该用户。

为了提供进一步的安全性，认证服务器 250 可以基于用户名、访问号码以及一条或多条附加信息来认证该用户，诸如对于用户独特的密码、对于用户独特的生物量测信息、对于一组用户独特的密码（例如，相同公司的雇员）、对于由用户使用的计算机设备 240 独特的地址或可以独特地或半独特地识别用户的某种其他信息。

访问号码可以以多种方式提供给认证服务器 250。例如，用户可以使用诸如键盘的输入设备来输入访问号码。替代地，访问号码可以经由有线或无线连接直接或间接地从电话设备 210 传送至计算机设备 240。

用户可以基于访问号码被认证（框 470）。例如，如上所述，认证服务器 250 可以从用户搜集信息，并且认证该用户。在一种实施方式中，如上所述，认证服务器 250 可以基于用户名和有效访问号码来适当地认证该用户。当访问号码与从服务提供商服务器 220 接收到的访问号码相匹配，并且该访问号码在到期之前被接收到时，该访问号码可以被认为有效。在另一实施方式中，如上所述，认证服务器 250 可以使用附加信息来适当地认证该用户。在访问号码使用之后，认证服务器可以立即使之到期。在该情形下，如果用户随后试图使用相同访问号码向认证服务器认证，则认证服务器 250 将不会适当地认证该

用户，因为该访问号码将被识别为无效。

可以提供对受限资源 260 的选择性访问权（框 480）。例如，如果认证服务器 250 无法适当地认证该用户，那么认证服务器 250 可以拒绝用户对受限资源 260 的访问。在该情形下，用户可能需要再次呼叫服务提供商服务器 220，以获取新的访问号码（例如，框 410）。如果认证服务器 250 适当地认证了该用户，那么认证服务器 250 可以授予用户对受限资源 260 的访问权。在该情形下，认证服务器 250 可以将消息发送至受限资源 260，或管理对受限资源 260 的访问的另一设备（例如，防火墙、网关等），以允许该用户的访问权。基于与受限资源 260 相关联的策略，用户对受限资源 260 的访问权可以是不受限的（例如，允许对受限资源 260 的任何部分的不受限访问）或受限的（例如，仅允许对受限资源 260 的某个（些）部分的访问）。

在一个替代实施方式中，由服务提供商服务器 220 提供的访问号码可以不包括嵌入其中的用户识别信息（或电话识别信息）。在该情形下，认证服务器 250 可以基于用户名、访问号码以及诸如密码或生物量测数据的对于用户独特的其他信息来认证用户。

在又一实施方式中，服务提供商服务器 220 可以仅基于电话识别信息来认证用户。在该情形下，认证服务器 250 可以基于用户名、访问号码以及诸如密码或生物量测数据的对于用户独特的其他信息来认证该用户。

图 7 是其中可以实现此处所描述的系统和方法的另一网络 700 的示例性视图。网络 700 可以包括经由网络 230 连接至服务提供商服务器 220 的电话设备 210，以及经由网络 270 连接至受限资源 710-730 的计算机设备 240。电话设备 210、服务提供商服务器 220、网络 230、计算机设备 240 以及网络 270 可以被配置成与关于图 2 描述的相同元件类似。

虽然在图 7 中未示出认证服务器 250，但是可以假定对于每个公司或每个受限资源（未示出）都存在认证服务器。替代地，认证服务器的功能可以嵌入受限资源 710-730 中。

如关于图 2 所描述的，受限资源 710-730 中的每个可以被配置成与受限资源 260 类似。虽然在图 7 中示出了三个受限资源 710-730，但是在实践中，可以存在更多或更少的受限资源。然而，假定在网络 700 中受限资源 710-730 与不同法律实体（例如，公司）相关联。如图 7 所示，受限资源 710 可以与公司 A 相关联，受限资源 720 可以与公司 B 相关联，并且受限资源 730 可以与公司 C 相关联。公司 A-C 中的每个可以预订由服务提供商服务器 220 提供的认证服务。

在该情形下，使用与关于图 4 的上述过程类似的过程，可以选择性地向用户提供对受限资源 710-730 的任何一个的访问权。结果，服务提供商服务器 220 能够将一个公司的受限资源的用户交叉认证至另一公司。这可以创建信赖相同认证源（例如，服务提供商服务器 220）的公司团体。这也可以允许交叉促销，以便公司 A 可以向公司 C 促销，使得公司 C 的客户可以使用他们当前对公司 C 所使用的相同认证程序来获得对公司 A 的受限资源的快速和安全访问权。

当用户访问服务提供商服务器 220 以获取访问号码时，服务提供商服务器 220 可以确定用户与哪一个或一些公司相关联。例如，用户可以既是公司 A 也是公司 B 的客户。在该情形下，当服务提供商服务器 220 将访问号码发送至用户时，服务提供商服务器 220 也可以将该访问号码提供至这两个公司，预期用户试图获得对与这两个公司中的一个相关联的受限资源的访问权。替代地，服务提供商服务器 220 可以识别用户与多个公司相关联，并且要求该用户选择该用户随后试图访问受限资源的公司中的一个。

图 8 是其中可以实现此处所描述的系统和方法的又一网络 800 的示例性视图。网络 800 可以包括经由网络 230 连接至服务提供商服务器 220 并且经由网络 270 连接至认证服务器 250 和受限资源 260 的用户设备 810。服务提供商服务器 220、网络 230、认证服务器 250、受限资源 260 和网络 270 可以被配置成与关于图 2 描述的相同元件类似。

用户设备 810 可以包括任何类型的通信或计算设备，诸如与电话设备 210 类似的电话设备、与计算机设备 240 类似的计算机设备或将电话设备和计算机设备的一些方面组合的设备。在网络 800 中，用户设备 800 可以不仅用于从服务提供商服务器 220 接收访问号码，而且用于使用该访问号码来访问受限资源 260。换言之，用户设备 810 可以联系服务提供商服务器 220，以获取访问号码。用户设备 810 可以随后联系认证服务器 250，并且使用该访问号码来获得对受限资源 260 的访问权。在这些实施方式中，独立的电话设备和计算机设备可以不是必需的。

此处所描述的实施方式可以提供一种用于向用户提供对受限资源的访问权的安全技术。

前面的描述提供了图示和描述，但并不意在穷尽或将本发明限于所公开的确切形式。各种修改和变更鉴于上述教导是可能的，或可以从本发明的实践中获取。

例如，虽然已经关于图 4 描述了一系列动作，但是在其他实施方式中，可以修改这些动作的顺序。而且，可以并行地执行非依附性动作。

而且，虽然已经描述了用户经由电话呼叫从服务提供商服务器 220 接收访问号码，但是并不必然是这种情形。在另一实施方式中，用户可以经由诸如即时消息的文本消息或另一可靠、快速的通信形式来接

收该访问号码。

而且，已经描述了经由认证服务器获得对受限资源的访问权。在另一实施方式中，服务提供商可以作为用于该受限资源的代理服务器而操作，以便用户可以通过该服务提供商服务器获得对该受限资源的访问权。

显而易见，如上所述，这些系统和方法可以以在图中所示的实现中的软件、固件和硬件的不同形式来实现。用于实现这些系统和方法的实际软件代码或专用控制硬件不限制本发明。因此，在没有参考具体软件代码的情况下描述了这些系统和方法的操作和性能，应当理解，软件和控制硬件可以被设计成实现基于此处的描述的系统和方法。

除非另有明确描述，在本申请中所使用的元件、动作或指令都不应当被解释为对本发明是关键的或必要的。而且，如在此处所使用的，不加数量词的项意在包含一个或多个项。在仅指一个项的情况下，使用术语“一个”或类似语言。而且，除非另有明确说明，短语“基于”意在表示“至少部分地基于”。

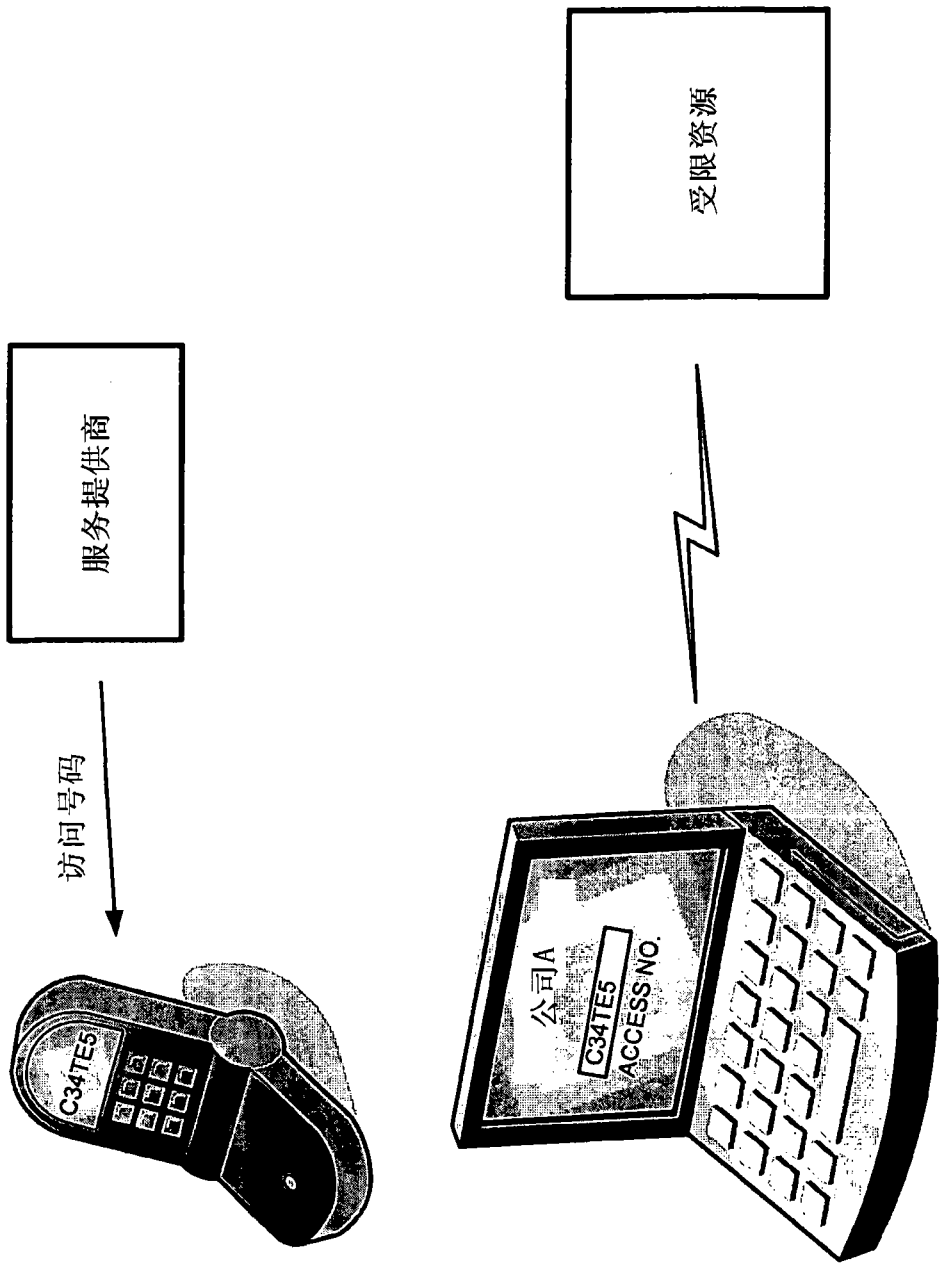


图1

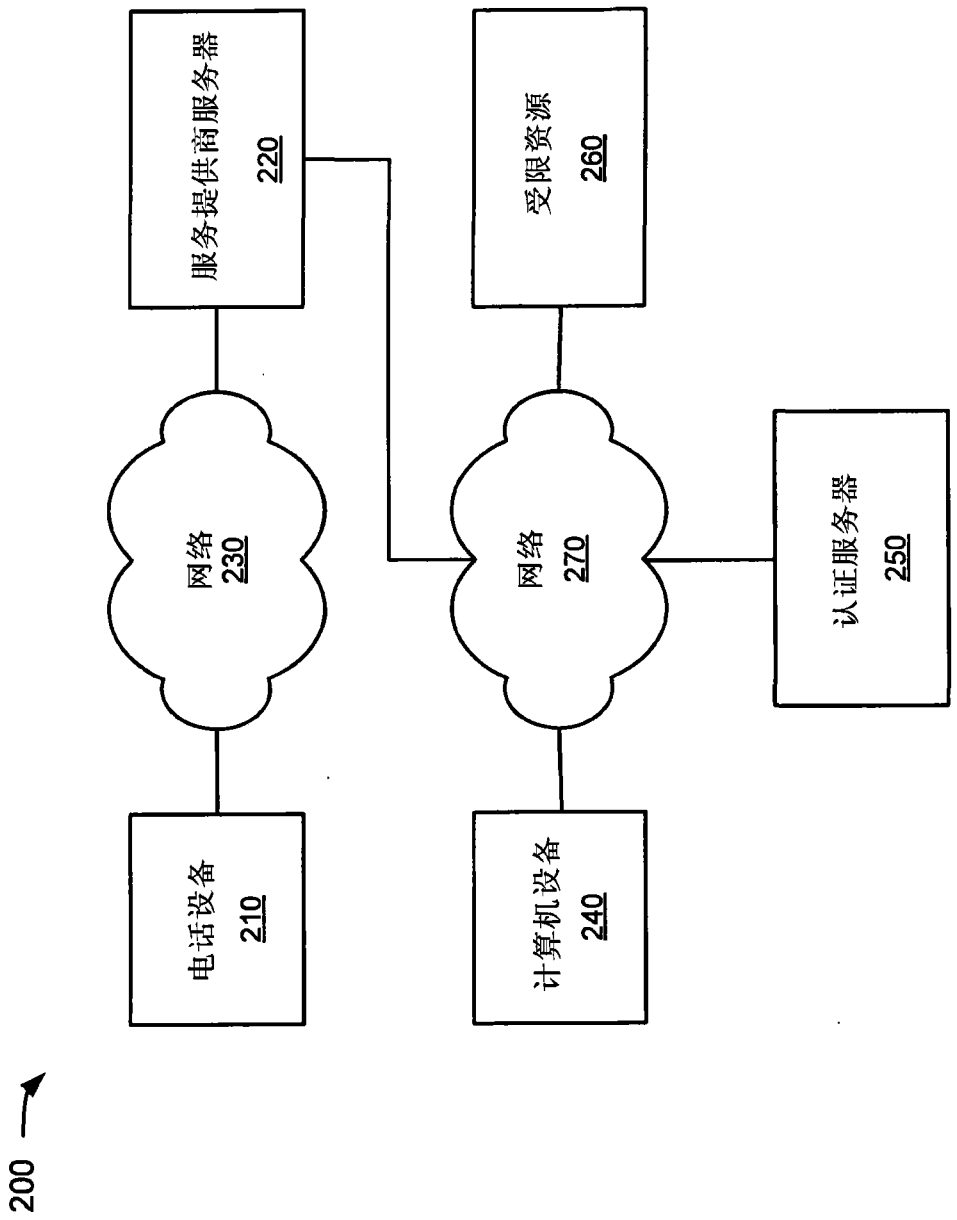

200
电话设备
210
网络
230
服务提供商服务器
220
计算机设备
240
网络
270
受限资源
260
认证服务器
250

图2

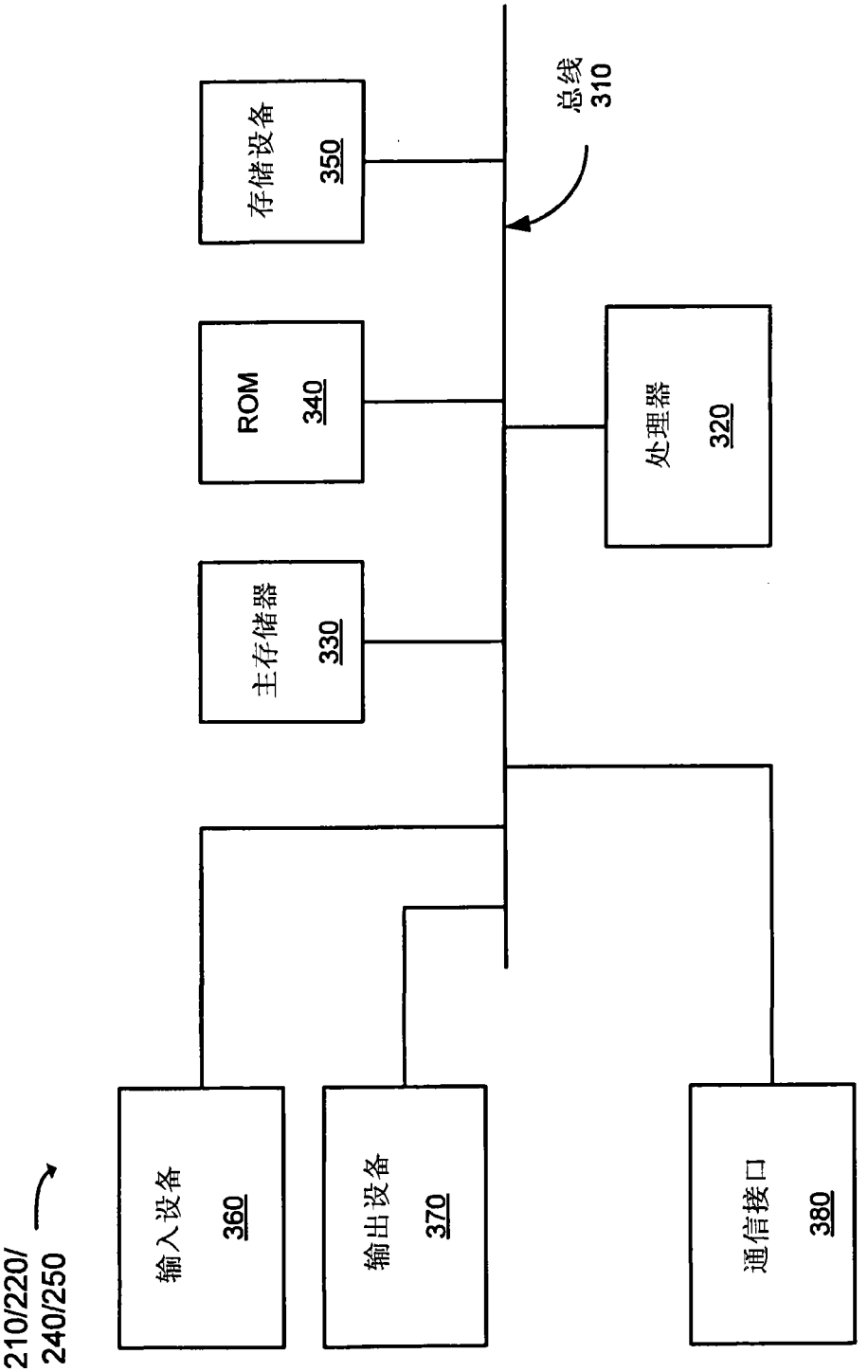

210/220/
240/250
输入设备
360
输出设备
370
通信接口
380
主存储器
330
ROM
340
存储设备
350
总线
310
处理器
320

图3

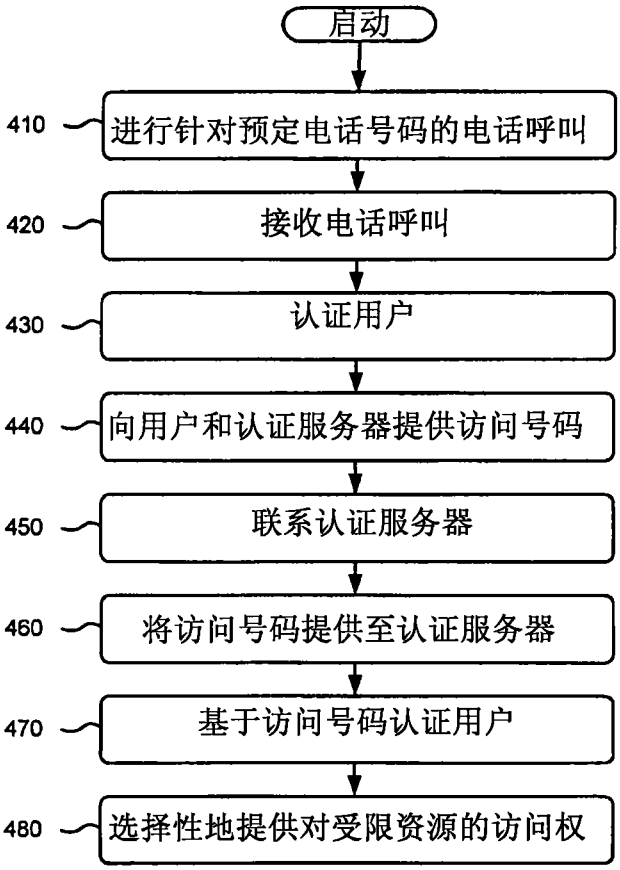

启动
410
进行针对预定电话号码的电话呼叫
420
接收电话呼叫
430
认证用户
440
向用户和认证服务器提供访问号码
450
联系认证服务器
460
将访问号码提供至认证服务器
470
基于访问号码认证用户
480
选择性地提供对受限资源的访问权

图4



图5B

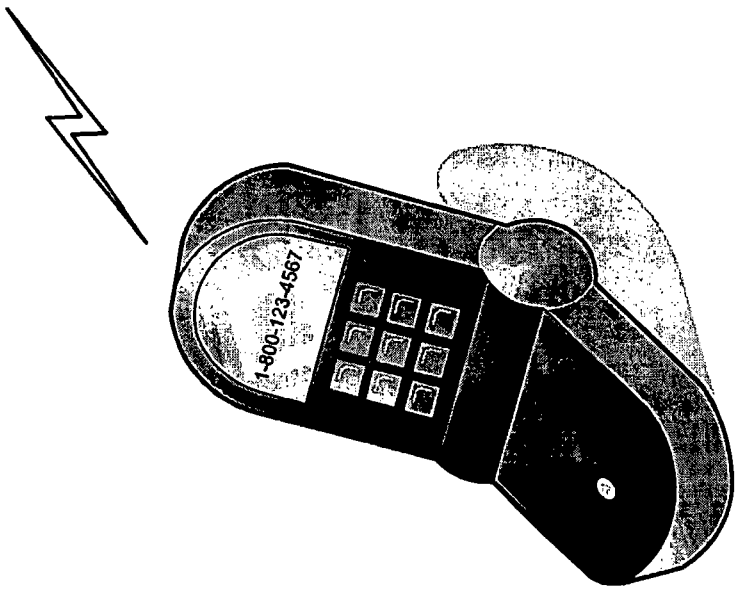


图5A

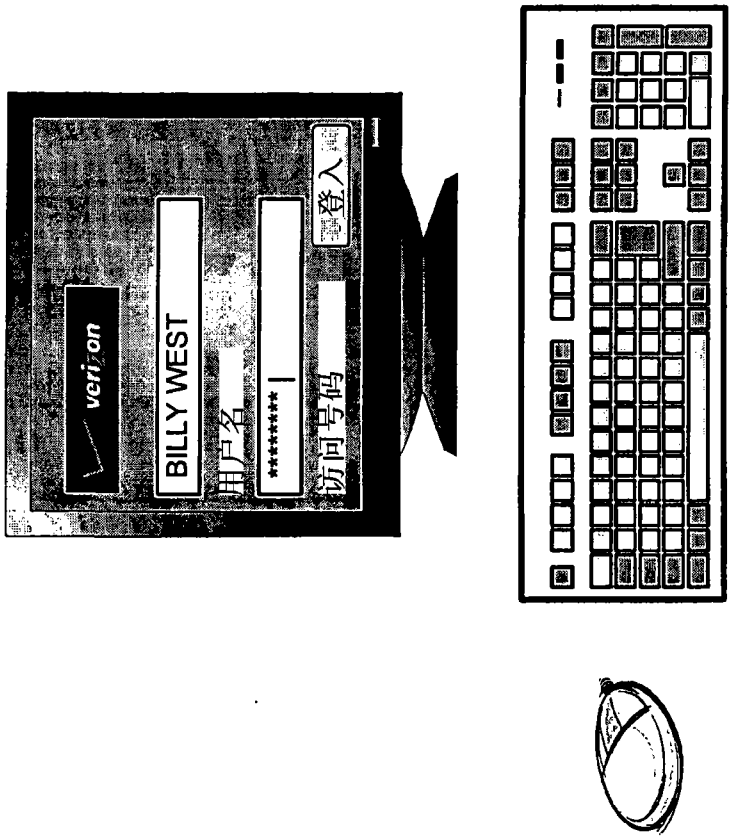


图6

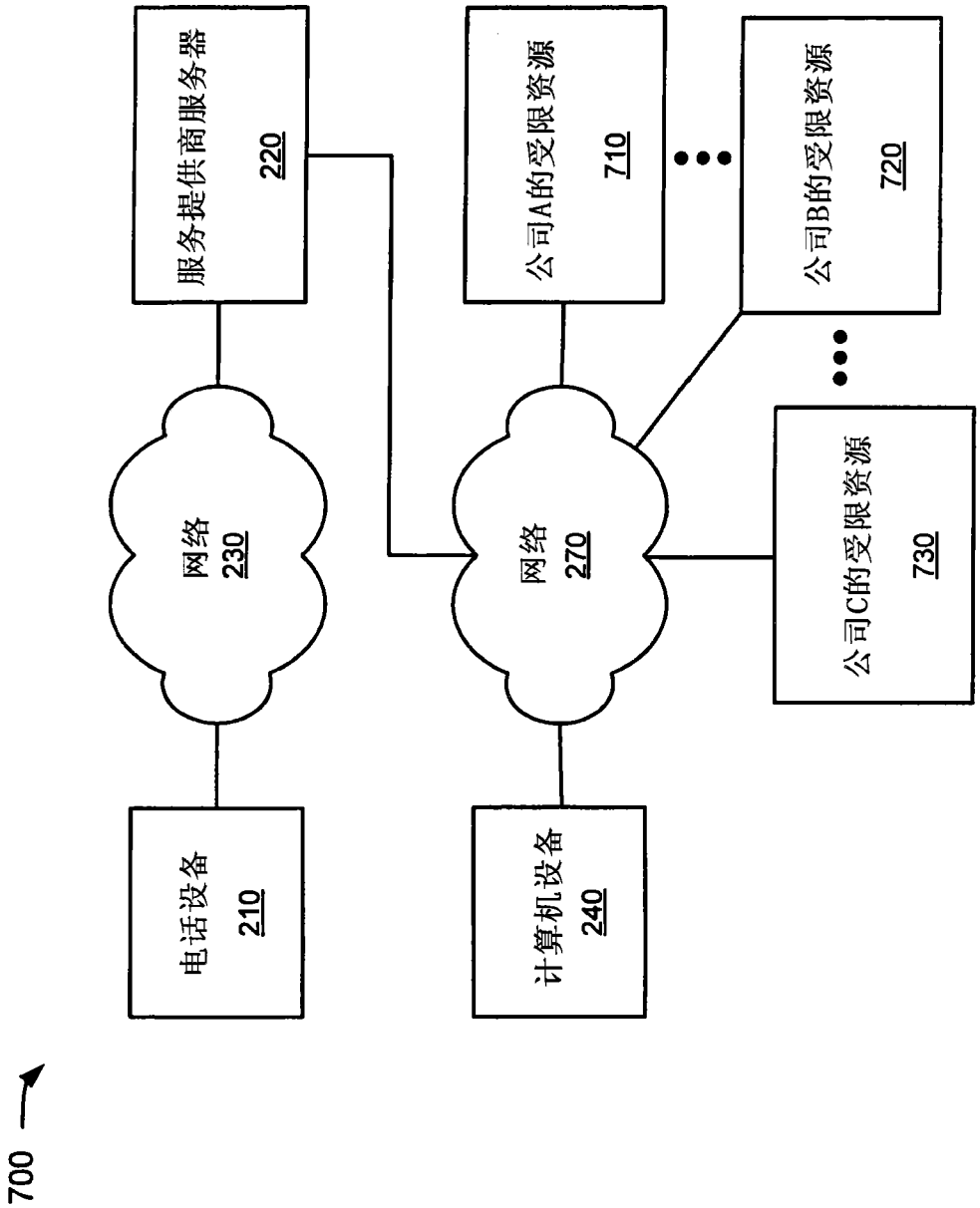

700
电话设备
210
网络
230
服务提供商服务器
220
计算机设备
240
网络
270
公司A的受限资源
710
公司B的受限资源
720
公司C的受限资源
730

图7

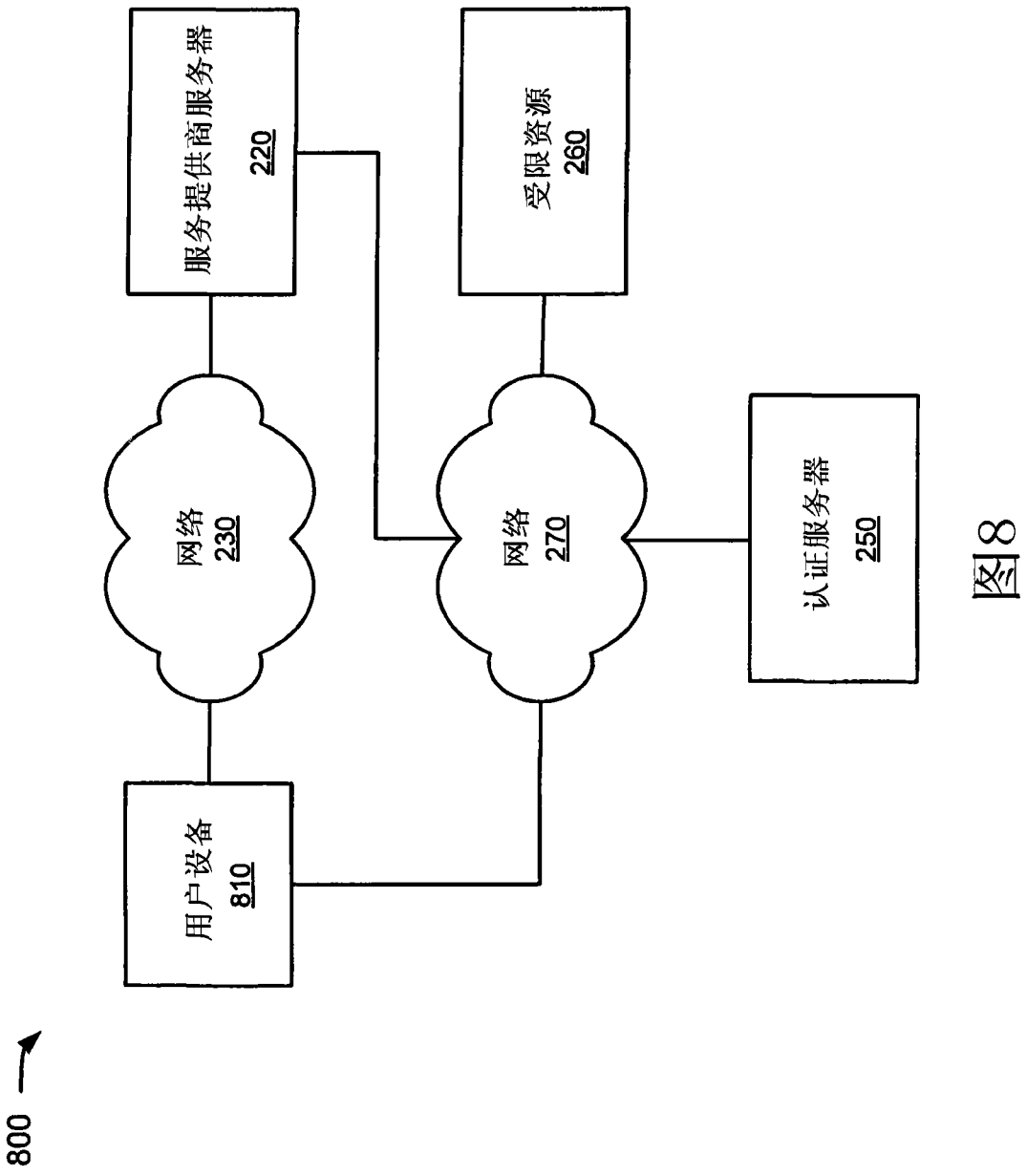


图8