(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 108351933 B
(45)授权公告日 2022.04.22

(21)申请号 201680061463.6

(22)申请日 2016.03.31

(65)同一申请的已公布的文献号
申请公布号 CN 108351933 A

(43)申请公布日 2018.07.31

(30)优先权数据
14/920,807 2015.10.22 US

(85)PCT国际申请进入国家阶段日
2018.04.20

(86)PCT国际申请的申请数据
PCT/US2016/025402 2016.03.31

(87)PCT国际申请的公布数据
WO2017/069800 EN 2017.04.27

(73)专利权人 甲骨文国际公司
地址 美国加利福尼亚

(72)发明人 S·马修 R·萨布拉曼亚
V·A·库泰伊

(74)专利代理机构 中国贸促会专利商标事务所有限公司 11038
代理人 张鑫

(51)Int.Cl.
G06F 21/44(2013.01)
H04L 9/40(2022.01)

(56)对比文件
US 2007136573 A1,2007.06.14
US 2014214688 A1,2014.07.31
US 2007199053 A1,2007.08.23
US 8555355 B2,2013.10.08
CN 103716326 A,2014.04.09
CN 102457484 A,2012.05.16
CN 104468119 A,2015.03.25
US 2007200597 A1,2007.08.30
Jim Youll.Fraud Vulnerability in Sitekey Security at Bank of America.《Review draft to Bank of America/RSA》.2016,第1-15页.
Rachna Dhamija 等.Phish and HIPs: Human Interactive Proofs to Detect Phishing Attacks.《Human Interactive Proofs,Second International Workshop on HumanInteractive Proofs(HIP 2005)》.2005,127-141页.

审查员 宋梦玲

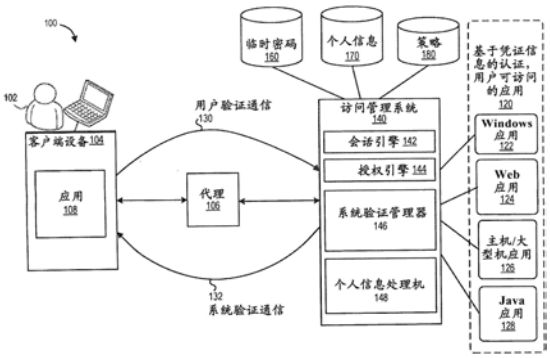
权利要求书3页 说明书27页 附图12页

(54)发明名称

用于最终用户启动的访问服务器真实性检查的方法和系统

(57)摘要

本公开涉及用于最终用户启动的访问服务器真实性检查的方法和系统。公开了用于使得用户能够验证计算系统(例如,访问管理系统)(诸如控制对一个或多个资源的访问的计算系统)的真实性的技术。用户可以在用户向访问管理系统提供凭证信息之前确定访问管理系统的真实性。可以在客户端系统处向用户呈现请求访问管理系统的认证的界面。访问管理系统可以在客户端系统处向用户提供临时访问信息以提交回访问管理系统。访问管理系统可以在客户端系统处向用户提供最近的个人信息以检验访问管理系统。在检验个人信息之后,访问管理系统可以提示用户输入凭证信息以建立会话。



CN 108351933 B

1.一种访问管理方法,包括:

由访问管理系统的计算系统从用户操作的计算设备接收验证请求以认证访问管理系统,所述验证请求包括与所述用户相关联的用户标识信息;

由所述计算系统基于所述用户标识信息向与所述用户相关联的目的地发送用于所述用户认证所述访问管理系统的临时访问信息;

由所述计算系统从所述计算设备接收包括所述临时访问信息的第一响应;

在检验在所述第一响应中接收到的所述临时访问信息后,由计算系统向所述计算设备发送关于所述用户的个人信息,所述个人信息选自能够从与所述访问管理系统不同的第三方系统获得的用户的当前记录;

从所述计算设备接收第二响应,所述第二响应指示所述用户对所述个人信息的确认,并且所述第二响应包括所述用户的凭证数据;以及

由计算系统确定所述用户从所述计算设备访问资源的认证,其中所述认证是基于在所述第二响应中接收到的所述凭证数据和对所述个人信息的确认来确定的。

2.如权利要求1所述的访问管理方法,还包括:

在确定所述用户未被认证从所述计算设备访问资源后,向所述计算设备发送对所述用户的凭证信息的请求;

其中所述计算设备响应于对凭证信息的请求而发送验证请求。

3.如权利要求1或2所述的访问管理方法,其中所述目的地包括所述计算设备。

4.如权利要求1或2所述的访问管理方法,其中所述目的地包括与所述用户相关联的设备,并且其中所述设备与所述计算设备不同。

5.如权利要求4所述的访问管理方法,其中所述第一响应是从所述目的地接收的。

6.如权利要求1或2所述的访问管理方法,还包括:

确定所述用户标识信息与所述用户相关联;以及

基于所述用户标识信息来识别所述目的地。

7.如权利要求1或2所述的访问管理方法,其中所述临时访问信息与时间段相关联,其中检验所述临时访问信息包括确定响应时间在所述时间段内,并且其中所述响应时间是基于在所述临时访问信息被发送到所述计算设备之后用于接收所述第一响应的时间的。

8.如权利要求1或2所述的访问管理方法,还包括:

在检验在所述第一响应中接收到的所述临时访问信息后,在发送所述个人信息之前生成所述个人信息。

9.如权利要求8所述的访问管理方法,其中所述个人信息包括在所述临时访问信息被检验之后确定的关于所述用户的财务信息。

10.一种访问管理系统,包括:

一个或多个处理器;以及

与所述一个或多个处理器耦合并且能够由所述一个或多个处理器读取的存储器,所述存储器存储一组指令,所述一组指令在被所述一个或多个处理器执行时使所述一个或多个处理器:

从由用户操作的计算设备接收验证请求以认证访问管理系统,所述验证请求包括与所述用户相关联的用户标识信息;

基于所述用户标识信息向与所述用户相关联的目的地发送用于所述用户认证所述访问管理系统的临时访问信息；

从所述计算设备接收包括所述临时访问信息的第一响应；

在检验在所述第一响应中接收到的所述临时访问信息后，将关于所述用户的个人信息发送给所述计算设备，所述个人信息选自能够从与所述访问管理系统不同的第三方系统获得的用户的当前记录；

从所述计算设备接收第二响应，所述第二响应指示所述用户对所述个人信息的确认，并且所述第二响应包括所述用户的凭证数据；以及

确定所述用户从所述计算设备访问资源的认证，其中所述认证是基于在所述第二响应中接收到的所述凭证数据和对所述个人信息的确认来确定的。

11.如权利要求10所述的访问管理系统，其中所述一组指令在被所述一个或多个处理器执行时还使所述一个或多个处理器：

在确定所述用户未被认证从所述计算设备访问资源后，向所述计算设备发送对所述用户的凭证信息的请求；

其中所述计算设备响应于对凭证信息的请求而发送验证请求。

12.如权利要求10或11所述的访问管理系统，其中所述目的地包括与所述用户相关联的设备，并且其中所述设备与所述计算设备不同。

13.如权利要求10或11所述的访问管理系统，其中所述一组指令在被所述一个或多个处理器执行时还使所述一个或多个处理器：

确定所述用户标识信息与所述用户相关联；以及

基于所述用户标识信息识别所述目的地。

14.如权利要求10或11所述的访问管理系统，其中所述临时访问信息与时间段相关联，其中检验所述临时访问信息包括确定响应时间在所述时间段内，并且其中所述响应时间是基于在所述临时访问信息被发送到所述计算设备之后用于接收所述第一响应的时间的。

15.如权利要求10或11所述的访问管理系统，其中所述一组指令在被所述一个或多个处理器执行时还使所述一个或多个处理器：

在检验在所述第一响应中接收到的所述临时访问信息后，在发送所述个人信息之前生成所述个人信息，其中所述个人信息包括在所述临时访问信息被检验之后确定的关于所述用户的财务信息。

16.一种存储一组指令的非瞬态计算机可读介质，所述一组指令在被一个或多个处理器执行时使所述一个或多个处理器：

由访问管理系统的计算系统从用户操作的计算设备接收验证请求以认证访问管理系统，所述验证请求包括与所述用户相关联的用户标识信息；

由所述计算系统基于所述用户标识信息向与所述用户相关联的目的地发送用于所述用户认证所述访问管理系统的临时访问信息；

由所述计算系统从所述计算设备接收包括所述临时访问信息的第一响应；

在检验在所述第一响应中接收到的所述临时访问信息后，由所述计算系统将关于所述用户的个人信息发送给所述计算设备，所述个人信息选自能够从与所述访问管理系统不同的第三方系统获得的用户的当前记录；

从所述计算设备接收第二响应，所述第二响应指示所述用户对所述个人信息的确认，并且所述第二响应包括所述用户的凭证数据；以及

由所述计算系统确定所述用户从所述计算设备访问资源的认证，其中所述认证是基于在所述第二响应中接收到的所述凭证数据和对所述个人信息的确认来确定的。

17.如权利要求16所述的非瞬态计算机可读介质，其中所述一组指令在被所述一个或多个处理器执行时还使所述一个或多个处理器：

在确定所述用户未被认证从所述计算设备访问资源后，向所述计算设备发送对所述用户的凭证信息的请求；

其中所述计算设备响应于对凭证信息的请求而发送验证请求。

18.如权利要求16或17所述的非瞬态计算机可读介质，其中所述目的地包括与所述用户相关联的设备，并且其中所述设备与所述计算设备不同。

19.如权利要求16或17所述的非瞬态计算机可读介质，其中所述一组指令在被所述一个或多个处理器执行时还使所述一个或多个处理器：

确定所述用户标识信息与所述用户相关联；以及

基于所述用户标识信息识别所述目的地。

20.如权利要求16或17所述的非瞬态计算机可读介质，其中所述一组指令在被所述一个或多个处理器执行时还使所述一个或多个处理器：

在检验在所述第一响应中接收到的所述临时访问信息后，在发送所述个人信息之前生成所述个人信息，其中所述个人信息包括在所述临时访问信息被检验之后确定的关于所述用户的财务信息。

用于最终用户启动的访问服务器真实性检查的方法和系统

[0001] 相关申请的交叉引用

[0002] 本申请要求于2015年10月22日提交的标题为“END USER INITIATED ACCESS SERVER AUTHENTICITY CHECK”的美国非临时专利申请No.14/920,807的权益和优先权，该申请的全部内容通过引用被结合于此用于所有目的。

技术领域

[0003] 一般而言，本申请涉及数据处理。更具体而言，本申请涉及用于使得用户能够验证控制对资源的访问的计算系统的真实性的技术。

背景技术

[0004] 现代企业依赖各种控制和生成对商业运营至关重要的信息的应用和系统。不同的应用常常提供不同的服务和信息，并且不同的用户可以需要访问每个系统或应用内的不同级别的信息。用户被授予的访问级别可以取决于用户的角色。例如，经理可以需要访问关于向其报告的员工的某些信息，但是让那个经理访问关于他向其报告的人的相同信息可能不恰当。

[0005] 之前，较不复杂的应用将访问管理业务逻辑直接结合到应用代码中。即，例如，每个应用将需要用户拥有单独的账户、单独的策略逻辑和单独的权限。此外，当用户通过这些应用之一进行认证时，这种认证对于企业中的其它应用仍然未知，因为关于第一应用的认证已发生的事实不共享。因此，在使用不同系统进行认证和访问控制的应用之间没有信任概念。工程师们很快意识到，为企业中的每个应用设置访问管理系统就像为每辆车配备加油站，并且确定认证和访问控制将作为共享资源更高效地被实现和管理。这些共享资源被称为访问管理系统。

[0006] 访问管理系统常常使用策略和其它业务逻辑来确定是否应当将特定访问请求授予特定资源。在确定应当授予访问之后，向请求者提供令牌。这个令牌就像钥匙，可以用来打开保护受限数据的门。例如，用户可以尝试访问人力资源数据库以搜集关于某些员工的信息(诸如工资信息)。用户的web浏览器向应用发出请求，该请求需要认证。如果web浏览器没有令牌，那么会要求用户登录访问管理系统。当用户通过认证时，用户的浏览器接收表示可用于访问人力资源应用的令牌的cookie。

[0007] 在企业中，用户(例如，员工)通常可以访问一个或多个不同的系统和应用。这些系统和应用中的每一个可以利用不同的访问控制策略并且需要不同的凭证(例如，用户名和密码)。单点登录(SSO)可以在初次登录之后为用户提供对多个系统和应用的访问。例如，当用户登录他们的工作计算机时，用户也可以访问一个或多个其它资源(诸如系统和应用)。访问管理系统可以质询用户，以检验他/她的身份，以确定对资源的访问。用户可以被质询基于“你拥有什么”、“你知道什么”和“你是谁”的组合的信息。

[0008] 访问管理系统可以利用客户端设备上的图形用户界面来提示用户，以询问用户信息来检验用户的凭证。有时候，用户请求的信息可以包括敏感的机密信息，如果包括这些信

息,那么可能威胁到个人的身份和个人信息(例如,财务信息或账户信息)。因此,用户在不确信请求该信息的系统是否确实控制对那些资源的访问的情况下可能会犹豫是否向系统(诸如服务器)提供敏感信息以获得对资源的访问。

[0009] 随着持续的使用诸如欺诈和网络钓鱼等技术的身份盗用的基于技术的进步,用户甚至更不愿意在无法检验凭证请求的来源的情况下提供他们的凭证。例如,访问管理系统可以向用户提供私人信息,以让用户基于私人信息来确定访问管理系统的真实性。但是,在这种情景下,欺诈和网络钓鱼系统可能会访问可用于诱使用户认为请求认证的系统是合法的个人信息。在另一个示例中,访问管理系统可以用特殊代码联系另一个设备以进行附加的检验。但是,欺诈系统可以访问用户的联系人信息,并且可以使用这些信息来发送附加的检验信息。在还有的另一个示例中,网络钓鱼或欺诈系统可以通过未被访问管理系统控制的收集页面获取凭证信息来试图欺骗用户。在一种情景下,在客户端系统上,恶意浏览器插件可能被激活以充当访问管理系统来错误地从用户请求访问凭证。

[0010] 在一些情况下,客户端系统可以接收一次性代码(例如,密码),以使得操作客户端系统的用户能够经由访问管理系统访问资源。客户端系统如果被危及或被盗,那么可以使得操作客户端系统的用户能够使用一次性代码获得对资源的未授权的访问。用于身份盗窃的一些技术可以用于拦截由用户操作的客户端系统与访问管理系统之间的通信。拦截的通信可以用于从用户恳求身份或访问信息。

[0011] 访问管理解决方案可能面临向用户提供使得用户能够启动对提供访问管理设施的系统的验证的能力的挑战。期望新技术来使得用户能够确定请求凭证信息访问资源的系统的真实性。

发明内容

[0012] 本公开一般而言涉及管理对资源的访问。公开了用于使得用户能够验证计算系统(例如,访问管理系统)(诸如控制对一个或多个资源的访问的计算系统)的真实性的某些技术。具体而言,公开了用于使得用户能够在用户向访问管理系统提供凭证信息之前确定访问管理系统的真实性的技术。

[0013] 本文公开的实施例使得用户能够使用信息来检验访问管理系统的真实性。每次信息可能不同,并且用户可以使用这些最新信息来检验访问服务器的真实性。访问管理系统和客户端系统之间的数据交换可以被模拟为最终用户和访问管理系统之间的三次握手。因此,访问管理系统不需要泄露任何机密信息,除非用户利用临时数据证明自己。本文描述的技术通过向用户询问临时数据(“你拥有什么”)和密码(“你知道什么”)来防止使用被盗卡或移动设备所暴露的安全风险。三次握手确保了认证从最终用户和从访问服务器端的角度看是完美无瑕的。

[0014] 在一些实施例中,可以在客户端系统处向用户呈现使得用户能够请求访问管理系统的认证的界面,诸如图形用户界面(GUI)。该界面可以在从用户请求访问由访问管理系统控制的资源的凭证信息之前呈现。通过检验访问管理系统的真实性,可以确保用户不将凭证信息提供给由未授权用户控制的计算系统。通过使得用户能够验证访问管理系统的真实性,用户可以确保凭证信息和其它机密信息不会被未授权方或实体破坏。还可以确保用户访问管理系统本身没有受到破坏,使得在提供凭证时,这些凭证的接收者可以获得对期望

资源的未授权访问。

[0015] 在本发明的一个方面中，请求系统验证的界面可以要求用户的标识信息以启动系统验证。标识信息可以使得访问管理系统能够识别用户以确定用于传送验证信息的联系人信息。联系人信息可以对应于作为系统验证的一部分访问管理系统可以与之通信的一个或多个目的地(例如，电子邮件地址或不同设备)。

[0016] 在系统验证期间，访问管理系统可以发送受一个或多个标准(诸如时间)约束的临时数据(例如，临时访问信息)。临时访问信息可以被发送到请求系统验证的客户端系统和/或与用户相关联的任何目的地。访问管理系统可以作为系统验证处理的一部分经由界面请求临时访问信息。访问管理系统可以检验临时数据以确定它是否与发送给用户的数据匹配。

[0017] 在检验临时数据与先前发送给用户的数据匹配之后，访问管理系统可以将个人信息发送给用户作为系统验证的一部分。个人信息可以包括未授权用户可能不知道的敏感的机密信息(例如，当前财务信息)。个人信息可以被发送到与用户相关联的客户端系统和/或(一个或多个)目的地。通过界面，用户可以指示个人信息是否正确。机密信息可以是只有用户和访问管理系统才知道的信息。机密信息可以包括对于其它外部计算机系统如果不是不可能那么也是不太可能被欺诈性地拦截、猜测或获取的信息。

[0018] 通过界面，用户可以在检验个人信息时提供凭证信息。凭证信息可以用于确定用户的认证作为系统验证处理的一部分。在基于凭证成功验证用户之后，访问管理系统可以为用户建立会话以使得能够访问资源。

[0019] 在一些实施例中，访问管理系统可以包括被配置为实现本文描述的方法和操作的计算系统。还有的其它实施例涉及采用或存储用于本文描述的方法和操作的指令的系统和机器可读的有形存储介质。

[0020] 在至少一个实施例中，一种方法可以包括从用户操作的计算设备接收验证请求以认证访问管理系统，该验证请求包括与用户相关联的用户标识信息。该方法可以包括基于用户标识信息向与用户相关联的目的地发送用于用户认证访问管理系统的临时访问信息。目的地可以是计算设备。目的地可以是与用户相关联的设备。设备可能与计算设备不同。该方法可以包括从计算设备接收包括临时访问信息的第一响应。该方法可以包括，在检验第一响应中接收到的临时访问信息之后，由计算系统向计算设备发送关于用户的个人信息。该方法可以包括从计算设备接收第二响应，第二响应指示用户对个人信息的确认，并且第二响应包括用户的凭证数据。该方法可以包括确定用户从计算设备访问资源的认证。认证可以基于在第二响应中接收到的凭证数据和个人信息的确认来确定。

[0021] 在一些实施例中，该方法可以包括在确定用户未被认证从计算设备访问资源之后，向计算设备发送对用户的凭证信息的请求。计算设备可以响应于对凭证信息的请求而发送验证请求。

[0022] 在一些实施例中，可以从目的地接收第一响应。

[0023] 在一些实施例中，该方法可以包括确定用户标识信息与用户相关联；并且基于用户标识信息来识别目的地。

[0024] 在一些实施例中，临时访问信息与时间段相关联。检验临时访问信息可以包括确定响应时间在该时间段内。响应时间可以基于在临时访问信息被发送到计算设备之后用于

接收第一响应的时间。

[0025] 在一些实施例中，该方法可以包括在检验第一响应中接收到的临时访问信息之后，在发送个人信息之前生成个人信息。

[0026] 在一些实施例中，个人信息包括在检验临时访问信息之后确定的关于用户的财务信息。

[0027] 通过参考以下说明书、权利要求书和附图，前述内容以及其它特征和实施例将变得更加明显。

附图说明

[0028] 下面参考以下附图详细描述本发明的说明性实施例：

[0029] 图1图示了根据实施例的用于使得用户能够验证访问管理系统的真实性的系统的高级图。

[0030] 图2图示了根据实施例的用于使得用户能够验证访问管理系统的真实性的系统的高级图。

[0031] 图3-4图示了根据实施例的示出用于使得用户能够验证访问管理系统的真实性的操作的序列图。

[0032] 图5描绘了根据实施例的图示用于使得用户能够验证访问管理系统的真实性的处理的流程图。

[0033] 图6-9图示了根据实施例的用于使得用户能够验证访问管理系统的真实性的处理的图形用户界面(GUI)。

[0034] 图10描绘了用于实现实施例的分布式系统的简化图。

[0035] 图11图示了根据本公开的实施例的其中服务可以作为云服务提供的系统环境的一个或多个部件的简化框图。

[0036] 图12图示了可以用于实现本发明的实施例的示例性计算机系统。

具体实施方式

[0037] 在以下描述中，为了说明的目的，阐述了具体的细节，以便提供对本发明的实施例的透彻理解。但是，显而易见的是，各种实施例可以在没有这些具体细节的情况下实践。例如，电路、系统、算法、结构、技术、网络、处理和其它部件可以以框图形式示为部件，以免用不必要的细节混淆实施例。附图和描述不旨在是限制性的。

[0038] 本公开一般而言涉及提供单点登录(SSO)访问。基于凭证信息(例如，用户名和密码)的认证，SSO会话可以在初始认证之后向用户提供对一个或多个系统的访问。对系统的访问可以提供对一个或多个资源的访问。资源可以包括由计算系统管理和/或存储的任何项目，诸如应用、文档、文件、电子内容等。资源可以由统一资源定位符(URL)或指示资源的来源的其它数据识别。

[0039] 公开了用于使得用户能够验证计算系统(例如，访问管理系统)(诸如控制对一个或多个资源的访问的计算系统)的真实性的某些技术。具体而言，公开了用于使得用户能够在用户向访问管理系统提供凭证信息之前确定访问管理系统的真实性的技术。

[0040] 本文公开的实施例使得用户能够使用信息来检验访问管理系统的真实性。每次信

息可能不同，并且用户可以使用这些最新信息来检验访问服务器的真实性。访问管理系统和客户端系统之间的数据交换可以被模拟为最终用户和访问管理系统之间的三次握手。因此，访问管理系统不需要泄露任何机密信息，除非用户利用临时数据证明自己。本文描述的技术通过向用户询问临时数据(“你拥有什么”)和密码(“你知道什么”)来防止使用被盗卡或移动设备所暴露的安全风险。三次握手确保了认证从最终用户和从访问服务器端的角度看是完美无瑕的。

[0041] 公开了用于使得用户能够验证访问管理系统的真实性的一些实施例，诸如系统、方法和机器可读介质。图1图示了系统100，其中访问会话中可访问的资源的用户(例如，用户102)可以启动处理来验证访问管理系统140的真实性。用户可能期望验证访问管理系统或任何计算系统的真实性，以确保访问信息(例如，密码或机密信息)不会受到未授权系统的破坏。为了图示的目的，如本文描述的“会话”包括SSO会话；但是，会话可以包括使得能够访问用户的其它类型的会话。访问管理系统140可以提供对一个或多个资源的访问。访问管理系统140可以实现登录系统(例如，SSO系统)，其可以建立SSO会话以提供对一个或多个资源的SSO访问。

[0042] 资源可以包括但不限于文件、网页、文档、web内容、计算资源或应用。例如，系统100可以包括诸如应用120和/或通过那些应用120可访问的内容之类的资源。可以使用应用来请求和访问资源。例如，应用可以基于识别所请求的资源的URL来请求对来自资源服务器的网页的访问。资源可以由一个或多个计算系统提供，例如，在SSO系统中进行了用户102的认证之后提供对一个或多个资源的访问的资源服务器。

[0043] 可以向操作客户端设备(例如，客户端设备104)的用户102呈现接受输入以使得用户能够与访问管理系统(例如，访问管理系统140)交互的一个或多个界面。界面的示例可以包括参考图6-9描述的图形用户界面(GUI)。界面可使用在客户端设备104上执行的应用(例如，应用108)访问。在用户102启动与用于用户102的认证的访问管理系统140的访问处理之前，界面可以接收请求验证访问管理系统140的真实性的输入。当从用户102接收到验证访问管理系统140的请求时，访问管理系统140可以启动访问管理系统140和由用户102操作的客户端设备104通过其进行通信的处理以使得用户能够验证访问管理系统140。用户与访问管理系统140之间的通信使得访问管理系统140能够检验它正在与为用户建立访问的实际用户通信。通信在客户端设备和访问管理系统140之间建立三次握手，以在用户和访问管理系统之间建立用于认证的信任以向用户提供对资源的访问。

[0044] 访问管理系统140可以由计算系统实现。计算系统可以包括一个或多个计算机和/或服务器(例如，一个或多个访问管理器服务器)，其可以是通用计算机、专用服务器计算机(作为示例，包括PC服务器、UNIX服务器、中程服务器、大型计算机、机架式服务器，等等)、服务器场、服务器集群、分布式服务器，或任何其它适当的布置和/或其组合。访问管理系统140可以运行任何数量的操作系统或各种附加服务器应用和/或中间层应用，包括HTTP服务器、FTP服务器、CGI服务器、Java服务器、数据库服务器等。示例性数据库服务器包括但不限于可从Oracle、Microsoft等商购获得的那些数据库服务器。访问管理系统140可以使用硬件、固件、软件或其组合来实现。

[0045] 在一些实施例中，访问管理系统140可以由在数据中心中部署为集群的多个计算设备(例如，访问管理器服务器)实现，这允许可伸缩性和高可用性。多个这种具有访问管理

器服务器集群的地理上分散的数据中心可以被连接(有线或无线),以构成多数据中心(MDC)系统。MDC系统可以满足企业计算机网络内访问服务器的高可用性、负载分布和灾难恢复要求。MDC系统可以充当单个逻辑访问服务器,以支持针对访问管理系统140的SSO服务。

[0046] 访问管理系统140可以包括至少一个存储器、一个或多个处理单元(或(一个或多个)处理器)和存储器。(一个或多个)处理单元可以用硬件、计算机可执行指令、固件或其组合适当地实现。在一些实施例中,访问管理系统140可以包括若干子系统和/或模块。例如,访问管理系统140可以包括会话引擎142、授权引擎144、系统验证管理器146和个人信息处理机148,其中的每一个可以用硬件、在硬件上执行的软件(例如,程序代码、可由处理器执行的指令)或其组合来实现。在一些实施例中,软件可以存储在存储器(例如,非瞬态计算机可读介质)中、存储器设备上或某种其它物理存储器上,并且可以由一个或多个处理单元执行(例如,一个或多个处理器、一个或多个处理器核心、一个或多个GPU等等)。(一个或多个)处理单元的计算机可执行指令或固件实现可以包括以任何合适的编程语言编写以执行本文描述的各种操作、功能、方法和/或处理的计算机可执行指令或机器可执行指令。存储器可以存储可在(一个或多个)处理单元上加载和执行的程序指令,以及在这些程序的执行期间生成的数据。存储器可以是易失性的(诸如随机存取存储器(RAM))和/或非易失性的(诸如只读存储器(ROM)、闪存等等)。存储器可以使用任何类型的持久存储设备(诸如计算机可读存储介质)来实现。在一些实施例中,计算机可读存储介质可以被配置为保护计算机免受包含恶意代码的电子通信。计算机可读存储介质可以包括存储在其上的指令,所述指令在处理器上执行时执行本文描述的操作。

[0047] 图1示出了其中用户102可以在启动认证处理(例如,用户提交凭证信息)之前进行与访问管理系统140的通信以验证访问管理系统140的示例。在这个示例中,操作客户端设备104的用户102可以尝试访问诸如应用108的资源,例如,应用120中的任何一个或者可通过应用120访问的资源。在成功认证用户102的信息凭证之后,应用120可以被用户102访问。在应用120之一可被在客户端设备104处的用户102访问之前,用户102可以针对向用户102提供对应用120的访问的会话进行认证。客户端设备104可以通过从访问管理系统140请求访问来启动认证处理。认证处理可以包括显示一个或多个GUI以接收用户的凭证信息并向访问管理系统140提交认证的请求的客户端设备104。可以基于检验用户102的凭证信息来建立认证。

[0048] 在尝试访问应用时,用户102可以操作经由访问管理系统140管理对用户账户的访问的应用(例如,应用108)。例如,应用108是可以呈现GUI的访问管理应用,诸如在图6-9中所绘出的。使用应用108,用户102可以启动验证处理以确定访问管理系统140的真实性(即,访问管理系统140是否负责用户102的认证)。验证处理可以包括从客户端设备104到访问管理系统140的一个或多个通信130(“用户验证通信”)。验证处理可以包括从访问管理系统140到一个或多个客户端设备(例如,客户端设备104)的、与启动验证处理的用户相关联的一个或多个通信132(“系统验证通信”)。验证处理的一些实施例在下面进一步描述。

[0049] 客户端设备104和访问管理系统140之间的通信可以通过网关系统来接收。网关系统可以支持访问管理服务。例如,单点登录(SSO)网关可以实现一个或多个访问代理(诸如代理106(例如,web网关代理))以平衡和/或处理来自客户端和访问管理系统140的请求。

[0050] 在至少一个实施例中，验证处理可以由用户102在应用108中启动。应用108可以呈现提示用户102输入凭证信息的GUI。当用户不再被认证时，可以请求凭证信息。会话的缺失或会话的到期可以促使访问管理系统140向用户102请求用于受保护的资源的凭证信息。应用108可以呈现使得用户102能够在提供凭证信息之前请求验证访问管理系统140的GUI。在启动对系统验证的请求之后，可以从客户端设备104向访问管理系统140发送用户验证通信130(例如，系统验证请求)以启动访问管理系统140的验证。具体而言，系统验证可以确定处理访问管理系统140的认证的计算系统的真实性。

[0051] 在接收到系统验证请求之后，访问管理系统140的系统验证管理器146可以管理系统验证。系统验证管理器146可以确定用于用户102检验的临时访问信息(例如，一次性密码)。临时访问信息可以受一个或多个标准(例如，时间)的约束。临时访问信息的示例可以包括密码、代码、令牌、密钥或受一个或多个标准约束的其它信息。临时访问信息可以在接收到系统验证请求时生成，或者可以先前生成。访问管理系统140可以将临时访问信息存储在数据存储库160中(“临时密码”)。

[0052] 系统验证管理器146可以将系统验证通信132中的临时访问信息发送到客户端设备104，以由用户102接收。用户102可以操作客户端设备104以将用户验证通信130与临时访问信息一起发送到访问管理系统140。访问管理系统140可以检验用户返回的临时访问信息以确定它是否匹配先前发送给用户102的内容。

[0053] 访问管理系统140的个人信息处理机148可以生成可能仅由用户已知或可访问的个人信息。在一些实施例中，可以获得不是正被验证的访问管理系统的一部分的第三方来源(例如，财务系统或提供个人信息的系统)的个人信息。用户102可能先前已经向访问管理系统140注册，从而从一个或多个源(例如第三方系统)提供访问个人信息的信息。个人信息可以包括与用户相关联的最近信息，该最近信息不能以其它方式被不具有访问该信息的特权的未授权用户访问。个人信息可以存储在数据存储库中，例如，数据存储库170(“个人信息”)中。最近个人信息可以包括例如从当前财务记录(例如，银行记录)获得的财务信息。为了确保个人信息基于当前记录，个人信息处理机148可以在系统验证管理器146检验临时访问信息之后确定个人信息。

[0054] 系统验证管理器146可以将包括个人信息的系统验证通信132发送到客户端设备104。客户端设备104可以呈现显示个人信息的界面并且使用该界面，用户102可以指示个人信息是否正确。如果用户指示个人信息是正确的，则界面可以接受凭证信息以确定用户的认证。如果个人信息不正确，则用户可以如此指示并且可以选择不提供凭证信息。因此，个人信息的检验使得用户102能够确定访问管理系统140是否是真实的。如果个人信息不正确，则用户102可以确定访问管理系统140不是真实的，从而防止用户将凭证信息共享到可能未授权的计算系统。

[0055] 基于对凭证信息的成功认证，用户102可以访问资源(例如，应用120)。在接收到凭证信息之后，会话引擎142就可以检验所请求的资源(例如，应用170)是否是需要凭证来访问的受保护资源。会话引擎142可以请求授权引擎144确定对资源的访问是否受到保护。在确定对资源的访问未被保护时，会话引擎142可以准许访问资源。

[0056] 在确定对资源的访问受到保护时，会话引擎142可以基于凭证信息来确定用户102的认证。在确定用户102的认证之后，授权引擎144可以基于对用户102许可的访问来确定用

户102是否被授权访问资源。会话引擎142可以向客户端设备104发送通信以指示对资源的访问是否被用户102允许。基于访问是否被允许，应用108可以对用户102启用。

[0057] 访问管理系统140可以提供许多SSO服务，包括对资源的访问(例如，授予/拒绝访问)的管理、自动登录、应用密码的改变和重置、会话管理、应用凭证供应以及会话的认证。在一些实施例中，访问管理系统140可以为应用120(诸如运行或从客户端设备访问的**Windows®**应用、Web应用、**Java®**应用以及基于大型机/终端的应用)提供自动单点登录功能。如以上所解释的，访问管理系统120可以执行对操作客户端设备(例如，客户端设备104)的用户(例如，用户102)的认证。认证是通过其检验用户以确定他/她是他/她所宣称的人的处理。

[0058] 在一些实施例中，访问管理系统140可以使用存储在数据存储180(“策略”)中的一个或多个策略来控制对资源的访问。策略180可以包括认证策略，该认证策略指定要用于认证必须为其提供对给定资源的访问的用户的认证方法。策略180定义其中资源访问受保护的方式(例如，加密的类型等)。策略180可以包括指定用户或用户的组可以访问资源的条件的授权策略。例如，管理员只能授权组内的某些用户访问特定资源。访问管理系统140可以基于策略180中的一个或多个来确定SSO会话的认证。

[0059] 访问管理系统140还可以包括或耦合到附加的存储装置，该存储装置可以使用任何类型的永久性存储设备(诸如存储器存储设备或其它非瞬态计算机可读存储介质)来实现。在一些实施例中，本地存储装置可以包括或实现一个或多个数据库(例如，文档数据库、关系数据库或其它类型的数据库)、一个或多个文件存储库、一个或多个文件系统，或其组合。例如，访问管理系统140耦合到或包括用于存储诸如临时密码160、个人信息170和策略160之类的数据的一个或多个数据存储库。存储器和附加的存储装置都是计算机可读存储介质的示例。例如，计算机可读存储介质可以包括以用于存储信息(诸如计算机可读指令、数据结构、程序模块或其它数据)的任何方法或技术实现的易失性或非易失性、可移动或不可移动介质。

[0060] 会话引擎142可以处理处理，以确定是否存在让用户102访问资源的有效会话。会话引擎142检查让用户102访问受保护的请求资源的有效会话。会话引擎142可以基于对适用于用户102的一个或多个访问策略的考虑来评估用户102的会话的有效性。基于确定不存在用于用户102的有效会话，会话引擎102可以从用户102请求108凭证信息(“凭证”)。凭证信息的成功认证可以向用户提供对可以包括所请求的资源的一个或多个资源的访问。

[0061] 请求可以被传送到客户端设备104，客户端设备104作为响应提示用户102输入用户凭证，以确定会话的认证。请求可以包括到接收凭证信息的网页或用户界面(例如，网页、门户或表盘)的信息(例如，URL)。请求可以被传送到客户端设备104，客户端设备104作为响应提示用户102输入用户凭证以确定会话的认证。

[0062] 会话引擎142可以执行操作以认证用户102的凭证信息。在一些实施例中，会话引擎142可以存储关于在成功认证用户时建立的会话的信息。对于SSO会话(例如，SSO认证的会话)，可以将SSO会话作为SSO会话进行管理，该SSO会话使得能够基于对用户的凭证信息的成功认证来访问用户可访问的所有资源。

[0063] 在一些实施例中，会话引擎142可以与授权引擎144关于认证的范围进行通信。授权引擎210可以确定受保护的资源并且基于认证会话150可以确定对于会话被允许和/或限

制的资源。

[0064] 在一些实施例中,可以在系统100中根据用于在客户端设备104和为访问管理系统140实现的访问管理器服务器中的任何一个之间的通信的代理-服务器模型来实现访问管理系统140。代理-服务器模型可以包括代理部件(例如,网关系统)和服务器部件。代理部件可以被部署在主机系统上,并且服务器部件可以被部署在服务器上,例如,访问管理器服务器。操作客户端设备104的用户102可以使用企业计算机网络经由代理106与访问管理系统140通信。客户端设备104可以是工作站、个人计算机(PC)、膝上型计算机、智能电话、可穿戴计算机或其它联网的电子设备。

[0065] 代理106可以提供访问控制,并且可以操作来保护访问管理系统140和通过访问管理系统140可访问的任何资源免受外部和内部的基于web的威胁。访问管理系统140可以与提供对一个或多个资源(例如,应用120)的访问的一个或多个资源计算系统(例如,资源服务器)通信。代理106可以实现或操作为代理部件访问管理系统140,并且可以包括作为服务器部件操作的服务器。通过访问管理系统140可访问的每个资源可以通过代理(例如,代理106)来保护。代理106可以截取对由其保护的一个或多个资源的用户请求并检查用户凭证以便认证用户。代理然后可以联系服务器,例如访问管理系统140处的访问管理器服务器。访问管理服务器可以检验资源是否是需要凭证来访问的受保护资源。如果访问管理服务器确定资源是未受保护的,则代理106可以向用户102授权访问。如果资源是受保护的,则代理106可以请求用户102提供认证凭证。

[0066] 在一些实施例中,代理106和访问管理系统140之间的通信可以被分成两个不同的通信信道。例如,经由前端信道的通信可以使用超文本传输协议安全(HTTPS)协议。前端信道通信可以包括较不频繁的通信,诸如用于认证的凭证收集操作的通信。经由后端信道的通信可以使用开放式访问协议(OAP)。后端信道通信可以包括更频繁的通信,诸如包括访问由访问管理系统140管理的资源的请求的代理-服务器交互。每个信道可以使用针对该信道上的通信类型设计的访问令牌进行通信。访问流程可以生成两种类型的浏览器令牌。第一令牌是访问管理ID令牌(例如,OAM_ID令牌),其服务于通过HTTP传播的SSO请求。第二令牌是可以用于服务通过OAP传播的SSO请求的授权令牌(例如,OAMAuthn令牌)。浏览器令牌可以作为主机cookie存储在客户端设备104处。

[0067] 访问管理系统140(例如,使用代理106)可以以询问的形式(例如,经由客户端设备104处的用户的web浏览器)向用户102呈现对于认证凭证的请求。在一些实施例中,用户102可以通过在客户端设备104上执行的客户端或者通过客户端设备104上的web浏览器来访问SSO用户界面。SSO用户界面可以在访问管理系统140处实现。访问管理系统140可以与请求108一起发送SSO用户界面或使得能够访问SSO用户界面的信息(例如,URL)。

[0068] 在一些实施例中,SSO用户界面可以包括用户102通常使用的应用的列表。用户102可以通过SSO用户界面管理他们的与应用相关联的凭证和策略。当用户102通过SSO用户界面请求访问应用(例如,应用140)时,可以从客户端设备104向访问管理系统140发送请求,以根据适用于用户102的一个或多个策略160中确定应用的策略类型。访问管理系统140可以确定是否存在用于用户的有效会话,并且如果存在,那么它可以基于策略类型确定用户102的凭证信息。

[0069] 在一些实施例中,请求可以包括来自先前登录的认证cookie,其可以用于确定用

户102是否被授权检索凭证。如果被授权，那么用户可以使用凭证登录到应用中。在一些实施例中，代理106可以使得用户能够使用由访问管理系统提供的SSO服务来访问应用120。访问可以通过web浏览器直接提供，而无需首先访问SSO用户界面或使用在客户端设备104上执行的客户端。如果用户102未被授权，那么访问管理系统可以从用户102请求108凭证。SSO用户界面可以呈现接收包括凭证信息的输入的界面。凭证信息可以被发送110到访问管理系统140，以确定用户102的认证。

[0070] 在一些实施例中，可以支持凭证类型，诸如Oracle访问管理受保护资源、联合应用/资源和表格填写应用。凭证类型的示例可以包括智能卡/感应卡(Proximity card)、令牌、公钥基础设施(PKI)、Windows登录、轻量级目录访问协议(LDAP)登录、生物特征输入等。对于受OAM保护的资源，用户请求可以被认证，并且然后被引导到与所请求的资源相关联的URL。对于联合应用，可以提供到联合合作伙伴和资源(包括企业对企业(B2B)合作伙伴应用和SaaS应用)的链接。对于表单填写应用，可以使用模板来识别通过其可以提交凭证的应用网页的字段。

[0071] 在一些实施例中，接收用于提供认证凭证的输入的SSO用户界面可以包括一个或多个交互元素以启动系统验证。界面的示例可以包括参考图6-9描述的那些界面。

[0072] 现在转到图2，图示了系统200，其中用户102可以启动处理来验证访问管理系统140的真实性。图2中示出的示例可以包括图1的元素。在系统200所示的示例中，验证访问管理系统140的真实性可以通过访问管理系统140和启动访问管理系统140的验证的客户端设备104之间的一个或多个通信，以及通过访问管理系统140和一个或多个目的地(诸如客户端设备210)之间的一个或多个通信来促进。目的地可能不与客户端设备104物理上位于一处。目的地可以对应于诸如电子邮件地址或电话号码之类的位置，数据可以从该位置处传送和/或接收。操作客户端设备104的用户可以访问目的地，使得用户可以促进访问管理系统140的验证。目的地可以使得用户能够从访问管理系统140接收信息和/或将信息发送到访问管理系统140。

[0073] 与目的地的通信可以被认为是带外的，使得通信是与不位于客户端设备104处的设备和/或是使用不同于与客户端设备104通信的通信机制。与目的地的通信可以使得能够安全传送用于验证访问管理系统140的信息，以便防止未授权用户获得对用于访问管理系统140的验证的信息的访问。在至少一个实施例中，访问管理系统140的验证可以包括向一个或多个目的地(例如，客户端设备210)发送一个或多个通信202(“系统验证通信”)的访问管理系统140。访问管理系统140的验证可以包括向访问管理系统140发送一个或多个通信204(“用户验证通信”)的目的地。

[0074] 在至少一个示例中，访问管理系统140可以向客户端设备210发送一个或多个系统验证通信202以提供诸如临时访问信息和/或个人信息的信息作为访问管理系统140的验证的一部分。操作客户端设备104的用户可以访问目的地以向访问管理系统发送用户验证通信204来确认信息的接收。用户可以访问目的地以从访问管理系统140获得信息，并利用从目的地获得的信息从客户端设备104响应访问管理系统140。以这种方式，信息可以在访问管理系统140和用户之间以安全的方式通信，以减少(如果不是防止的话)未授权用户获取用于访问管理系统140的验证的信息。客户端设备104和目的地的使用进一步确保了用于验证的信息被接收和/或检验。在一些实施例中，诸如客户端设备210的目的地处的应用208可

以提供界面来促进用于访问管理系统140的验证的信息的通信。

[0075] 在一些实施例中，访问管理系统140可以支持注册处理，通过该注册处理，操作客户端设备104的用户可以注册用于访问管理系统140的验证的一个或多个目的地。注册可以包括存储关于目的地的信息。每个注册的目的地可以与注册目的地的用户的用户标识信息一起存储。访问管理系统140可以基于由用户提供的用户标识信息来识别目的地。用户可以为目的地指定一个或多个标准(例如，时间)，使得访问管理系统140可以根据标准与目的地通信。现在转到图3和图4，其中图示了访问管理系统140的验证的示例。

[0076] 在一些实施例中，诸如参考图3-9描述的那些实施例可以被描述为被描绘为被绘出为流程图、流图、数据流图、结构图、序列图或框图的处理。虽然序列图或流程图可以将操作描述为顺序处理，但是许多操作可以并行或并发地执行。此外，操作的次序可以被重新安排。处理在其操作完成时终止，但是可以具有图中不包括的附加步骤。处理可以与方法、函数、过程、子例程、子程序等对应。当处理与函数对应时，其终止可以与函数返回到调用函数或主函数对应。

[0077] 本文描述的处理(诸如参考图3-9描述的处理)可以用由一个或多个处理单元(例如，处理器核心)执行的软件(例如，代码、指令、程序)、硬件或其组合来实现。软件可以存储在存储器中(例如，在存储器设备上、在非瞬态计算机可读存储介质上)。在一些实施例中，在本文的流程图中绘出的处理可以由访问管理系统(例如，图1和图2的访问管理系统140)的计算系统来实现。本公开中的处理步骤的特定系列并不旨在进行限制。步骤的其它序列也可以根据替代实施例执行。例如，本发明的替代实施例可以以不同的次序执行上面概述的步骤。而且，图中所示的各个步骤可以包括多个子步骤，这些子步骤可以以对个体步骤适当的各种序列执行。虽然图3-9中绘出的处理可以关于访问单个资源来描述，但是可以针对多个资源来执行这样的处理，使得每当访问资源和/或需要确定用户对资源的访问的认证时，可以请求访问管理系统的计算系统的验证。图3-9中绘出的处理可以关于多个会话进行描述，可以针对每个会话请求访问管理系统的计算系统的验证。此外，取决于特定的应用，可以添加或去除附加的步骤。本领域普通技术人员将认识到许多变化、修改和替代。

[0078] 在一些实施例的一个方面，图3-9中的每个处理可以由一个或多个处理单元来执行。处理单元可以包括一个或多个处理器(包括单核或多核处理器)、处理器的一个或多个核，或其组合。在一些实施例中，处理单元可以包括一个或多个专用协处理器，诸如图形处理器、数字信号处理器(DSP)，等等。在一些实施例中，处理单元中的一些或全部可以使用定制电路(诸如专用集成电路(ASIC)或现场可编程门阵列(FPGA))来实现。

[0079] 图3-4图示了根据实施例的示出用于使得用户能够验证访问管理系统(例如，访问管理系统140)的真实性的操作的序列图。图3示出了用于使得用户能够从用户操作以访问一个或多个资源的客户端设备验证访问管理系统的真实性的序列图300。

[0080] 在步骤312处开始，用户操作客户端设备302以请求访问由访问管理系统管理访问的资源(“请求的资源”)。访问管理系统的会话引擎306可以被配置为管理对资源的访问。会话引擎306可以处理客户端设备302的认证以建立会话。会话引擎306可以在访问管理系统的服务器(例如，认证服务器)上实现。例如，会话引擎306可以包括或实现图1的会话引擎142。

[0081] 如上所述，资源可以是应用或使用应用可访问的资源。在图3的示例中，可以操作

客户端设备302以通过应用304请求对资源的访问。在步骤314处，应用304可以请求访问由客户端设备302请求的资源。应用304可以是通过与访问管理系统通信来管理访问的访问管理应用。用户可以经由应用304向访问管理系统提供访问凭证用于用户的认证。会话引擎306可以在成功认证用户之后建立会话(例如，SSO会话)。会话可以使得用户能够从客户端设备302访问一个或多个资源。

[0082] 在一些实施例中，访问资源的请求可以由诸如web网关之类的代理来处理。代理可以保护对服务器提供的资源的访问。客户端设备302可以通过直接或间接经由代理与会话引擎306通信来与访问管理系统140通信。代理可以截取对由其保护的一个或多个资源的用户请求以确定对所请求的资源的访问。代理可以检查用户凭证以便为访问由访问管理系统控制的那些资源的会话认证用户。代理可以确定资源是否受保护，如果是，那么确定是否存在活动会话以使得能够经由应用304从客户端设备302访问资源。

[0083] 会话引擎306可以处理客户端设备302的认证以建立会话。在接收到访问资源的请求时，在步骤320处，会话引擎306可以确定是否需要有效会话来访问资源。例如，会话引擎306可以确定对资源的访问是否受到保护。对资源的访问可以基于用户的认证。会话引擎306可以确定有效会话对于用户是否是活动的。有效会话的存在可以指示用户已被认证。会话引擎306可以确定活动会话是否使得能够访问资源，诸如所请求的资源。在一些实施例中，认证可以特定于某些资源。在一些实施例中，会话引擎306可以基于对适用于用户的一个或多个访问策略的考虑来评估用户的会话的有效性。

[0084] 在步骤322处，会话引擎306可以确定用户未被认证访问所请求的资源。会话引擎306可以通过确定不存在用于用户的有效会话来确定用户未被认证。在步骤330处，在确定用户未被认证访问资源之后，会话引擎306可以向客户端设备302发送对用户凭证信息的请求(“对用户凭证的请求”)。客户端设备302接收对凭证信息的请求。在一些实施例中，可以经由应用304接收来自步骤330的请求。

[0085] 响应于对用户凭证的请求，客户端设备302可以提供使得客户端设备能够接收凭证信息的界面。界面可以在应用中提供，例如应用304中。界面的示例在下面参考图6进行描述。界面可以包括一个或多个交互元素以使得用户能够请求正在请求用户的凭证的系统(例如，包括会话引擎306的访问管理系统)的验证。为了请求系统的验证，界面可以使得用户能够输入识别与请求相关联的用户的用户凭证(例如，用户标识信息)。如下面进一步描述的，会话引擎306可以使用用户标识信息来确定与系统的验证相关的通信的目的地。在步骤332处，客户端设备302可以接收对系统验证的请求。客户端设备302可以接收用户标识信息。在步骤340处，客户端设备302可以将对系统验证的请求发送到会话引擎306。该请求可以与用户标识信息一起发送。

[0086] 在步骤350处，会话引擎306可以确定请求系统验证的用户是否可以请求系统验证。会话引擎306可以开始系统验证处理以通过访问检验用户标识信息来验证访问管理系统。会话引擎306可以通过确定用户标识信息是否有效(例如，存在)，并且如果是，则确定它是否与用户相关联来检验用户标识信息。会话引擎306可以访问身份管理系统来检验用户标识信息。

[0087] 在会话引擎306检验用户标识信息(即，确定用户标识信息是有效的并且用户标识信息与用户相关联)之后，会话引擎306可以从身份管理系统接收与用户标识信息相关联的

通信首选项。通信首选项可以指示被指定为接收用于系统验证的临时访问信息的一个或多个目的地。会话引擎306可以与(一个或多个)目的地通信以提供临时访问信息。

[0088] 在步骤350处，会话引擎306可以为请求访问管理系统的系统验证的用户确定临时访问信息(例如，一次性密码)。临时访问信息可以用作系统验证处理的一部分。临时访问信息可以由访问管理系统生成和/或可以从第三方系统获得。在一些实施例中，临时访问信息可以在系统验证的请求之前生成。临时访问信息可以与将临时访问信息的使用限制在限制的时间段内的一个或多个约束相关联。

[0089] 在步骤352处，会话引擎306可以将临时访问信息发送给请求系统验证的用户。临时访问信息可以在基于用户的通信首选项识别出的一个或多个目的地处被发送给用户。如上所述，可以使用用户标识信息来检索通信首选项。在一些实施例中，目的地可以包括请求系统验证的客户端设备(例如，客户端设备302)。默认情况下(例如，当用户没有提供通信首选项时)，临时访问信息可以被发送到请求系统验证的客户端设备(例如，302)。临时访问信息可以使用一个或多个通信系统(例如，消息传送服务)传送给客户端设备。

[0090] 在步骤360处，请求系统验证的用户可以操作客户端设备302。用户可以操作客户端设备302以获得临时访问信息。客户端设备302可以提供具有接收临时访问信息的一个或多个交互元素的界面。用户可以操作客户端设备302以在界面中提供临时访问信息。客户端设备302接收提供到界面中的临时访问信息。在步骤362处，客户端设备302可以将临时访问信息发送到访问管理系统(例如，会话引擎306)以继续系统验证的处理。

[0091] 在步骤370处，会话引擎306可以检验临时访问信息。检验临时访问信息可以包括确定是否满足临时访问信息的约束。例如，在临时访问信息与时间限制相关联的情况下，会话引擎306可以基于时间限制来确定临时访问信息是否已经到期。当约束不满足时(即，当临时访问信息已经到期时)，临时访问信息不能被接受用于系统验证。在步骤352处，检验临时访问信息可以包括确定临时访问信息是否与发送给客户端设备302的临时访问信息匹配。临时访问信息可以与请求系统验证的用户的用户标识信息相关联地存储。

[0092] 还有，在步骤370处，会话引擎306可以确定个人信息作为系统验证的一部分。个人信息可以在检验临时访问信息时确定。个人信息可以由会话引擎306生成。在一些实施例中，可以获得不是正在被验证的访问管理系统的一部分的第三方来源(例如，财务系统)的个人信息。个人信息可以包括与用户相关联的最近信息，该最近信息不能以其它方式被不是用户标识信息的持有者的用户(例如，未授权用户)访问。最近信息可以包括例如从当前财务记录(例如，银行记录)获得的财务信息。为了确保个人信息基于当前记录，会话引擎306可以在检验临时访问信息时确定个人信息。

[0093] 在步骤372处，会话引擎306可以将个人信息发送到与请求系统验证的用户相关联的客户端设备。客户端设备可以是请求系统验证的设备。通过将个人信息发送到已知与用户相关联的客户端设备，确保会话引擎306个人信息不会被发送给未授权访问个人信息的用户。可以确保操作客户端设备302的用户个人信息来自被验证为授权访问管理系统的可信来源。在步骤380处，与请求系统验证的用户相关联的客户端设备可以显示个人信息以供用户检验。例如，个人信息可以在界面中显示。假设请求系统验证的客户端设备可能是接收个人信息的客户端设备。由于个人信息是作为系统验证的一部分由访问管理系统发送的，因此个人信息相对于请求系统验证的用户可能是准确的和当前的。个人信息可以基于在用

户请求的系统验证之后关于用户的个人信息的最近查询来确定。

[0094] 在步骤380处，客户端设备302可以向用户呈现使得用户能够提供输入以检验个人信息正确的界面。在检验个人信息正确之后，客户端设备302可以向用户呈现界面以接收与用户的用户标识信息对应的凭证信息。在检验个人信息准确之后，通过用户提交凭证信息可以完成系统验证处理。客户端设备302可以将凭证信息382发送到会话引擎306用于检验。

[0095] 在步骤390处，会话引擎306可以检验用户的凭证信息。检验凭证信息可以包括确定凭证信息是否匹配先前建立的与用户的用户标识信息相关联的凭证信息。在步骤312处访问所请求的资源可以基于检验凭证信息正确而被授权。在步骤392处，会话引擎306可以授权对所请求的资源的访问。可以通过存储指示访问被授权的信息来授权访问。会话引擎306可以向客户端302发送指示关于被授权的访问的信息的数据。在一些实施例中，关于被授权的访问的数据可以被发送到应用304。在步骤394处，应用304可以基于从会话引擎306接收到的指示访问已被授权的数据来使得能够访问资源(例如，应用304)。

[0096] 现在转到图4，示出了用于使得用户能够使用多个客户端设备验证访问管理系统的真实性的序列图400。具体而言，序列图400示出了访问管理系统的系统验证可以使用带外通信信道来促进。例如，参考图3描述的系统验证可以通过添加与物理上与客户端设备302分离的目的地410(“带外目的地”)的带外通信来增强。例如，目的地410可以是处于操作客户端设备302的用户的控制中并且与客户端设备302不同的客户端设备。目的地410可以是移动通信设备并且客户端设备302可以是台式计算机。带外通信可以通过防止或使未授权用户(例如，黑客或身份窃贼)更难以获得诸如个人信息和临时访问信息之类的敏感信息来提高系统验证处理的安全性。

[0097] 基于图3所示的示例，图4中的示例图示了与带外目的地的通信作为系统验证的一部分。带外目的地对于使得用户能够接收和/或发送重要通信作为系统验证的一部分而不会破坏通信中发送的信息是有用的。由于黑客可能不知道目的地，因此可以通过与目的地的通信来提高安全性。由此，黑客可能无法访问或拦截诸如个人信息和临时访问信息之类的信息。

[0098] 操作客户端设备302的用户可以在任何处理(诸如图3中和图4中绘出的系统验证)发生之前向访问管理系统注册。用户可以通过提供关于用户的信息来注册，包括关于用于系统验证的一个或多个目的地的信息。关于目的地的信息可以包括关于由用户控制的一个或多个客户端设备的设备信息和或关于其它类型的目的地的任何信息(例如，电子邮件账户信息)。关于用户的信息可以与用户标识信息和凭证信息相关联地存储。在一些实施例中，用户可以向访问管理系统可访问的身份管理系统注册信息。注册可以包括用户提供关于目的地的信息。访问管理系统可以经由启动系统验证的客户端设备和/或带外目的地中的一个或多个与用户通信以进行系统验证。

[0099] 图4中示出的示例可以包括与图3类似的元素。操作客户端设备302的用户可以请求访问由包括会话引擎306的访问管理系统控制的资源。作为获得对所请求的资源的访问的一部分，用户可以启动访问管理系统的系统验证。在启动系统验证之后，会话引擎306可以经由带外目的地410与用户通信以进行系统验证处理的一个或多个步骤。

[0100] 在一些实施例中，在步骤350处确定临时访问信息之后，会话引擎306可以将临时访问信息发送到与客户端设备302不同的一个或多个目的地。例如，在步骤452处，会话引擎

306可以将临时访问信息(例如,临时密码)发送到目的地410。除了向客户端设备302发送临时访问信息之外或作为其替代,会话引擎306可以向目的地410发送临时访问信息。在临时访问信息没有被发送到客户端设备302的情况下,操作客户端设备302的用户可能必须从目的地410获得临时访问信息。在步骤454处,目的地(如果是设备)可以将临时访问信息发送到客户端设备302,或者如果对用户可访问,则用户可以能够从目的地410获得临时访问信息。如上所述,临时访问信息由用户提供给访问管理系统作为系统验证处理的一部分。在图4中,在步骤360处,客户端设备302可以从用户作为输入接收或者在步骤454处从目的地410接收临时访问信息。

[0101] 在一些实施例中,作为系统验证的一部分,除了将个人信息发送到客户端设备302之外或作为其替代,访问管理系统可以将个人信息发送到一个或多个带外目的地(例如,目的地410)。例如,在步骤370处生成个人信息之后,会话引擎306可以将个人信息发送到目的地410。为了增强系统验证的安全性,可以将个人信息发送到带外目的地以防止未授权用户的访问。未授权用户可能不知道目的地的存在,并且即使如此,也可能不知道与系统验证处理相关的个人信息。在一些实施例中,可以在启动系统验证的客户端设备302和接收个人信息的一个或多个目的地之间共享个人信息。

[0102] 继续系统验证处理,无论何处接收到的个人信息可以由用户进行评估以确定其是否正确。在一些实施例中,系统验证处理可以包括提供界面(例如,图8中的界面)以使得用户能够提供输入以指示个人信息是否正确。界面可以在客户端设备302或目的地410处呈现给用户。在图4的示例中,可以在步骤380处向用户呈现界面。在步骤380处,客户端设备302可以在客户端设备302处经由界面接收指示对个人信息的检验的输入。

[0103] 因此,通过提供一个或多个目的地作为系统验证的一部分,可以确保用户访问管理系统在系统验证期间没有信息被未授权用户破坏。

[0104] 图5图示了根据实施例的用于使得用户能够验证访问管理系统的真实性的处理的流程图500。在一些实施例中,流程图500中绘出的处理可以由图1和图2的访问管理系统140来实现。

[0105] 流程图500可以在步骤502处通过确定用户是否被认证从客户端设备进行访问开始。例如,访问管理系统可以确定用户是否被认证以访问用户所请求的资源。可以确定对来自特定客户端设备(例如,用户请求访问的客户端设备)的访问的认证。可以基于由用户提供(例如,从用户操作的客户端设备接收到的)凭证信息(例如,用户标识和密码)来确定用户的认证。基于对凭证信息的检验,用户可以被认证从客户端设备进行访问。

[0106] 在一些实施例中,访问管理系统可以基于是否存在用于用户的有效会话(例如,SSO会话)来确定用户是否被认证。在确定有效会话存在之后,用户可以被认证。在一些实施例中,访问管理系统可以确定对于有效会话(如果存在的话),用户是否有权访问由用户请求的资源。

[0107] 在步骤504处,可以将请求发送到由用户操作的客户端设备。请求可以被发送用于用户的凭证信息以认证用户。在确定用户未被认证(例如,未被认证访问资源)之后,可以发送请求。

[0108] 在步骤506处,可以从客户端设备接收验证请求。验证请求可以被提交以请求访问管理系统的计算系统的验证。请求认证的计算系统可以是从用户请求认证信息的同一计算

系统。在一些实施例中，用户可以提交可以通过GUI(诸如下面参考图6进一步描述的GUI)提交的验证请求。GUI可以接收包括用户标识信息的输入。用户标识信息可以被包括在验证请求中。如下面进一步描述的，用户标识信息可以使得访问管理系统能够确定用于临时访问信息(例如，一次性密码)的通信的目的地。

[0109] 可以在步骤508处识别与用户相关联的目的地。可以基于验证请求(例如，在步骤506处接收到的验证请求)中的用户标识信息来识别目的地。用户标识信息可以包括唯一识别用户的用户标识(例如，用户名)或其它信息(例如，电话号码或电子邮件地址)。在一个示例中，访问管理系统可以从身份管理系统检索由用户标识信息识别出的用户的简档。目的地可以基于简档来识别，该简档指示用于与用户通信的一个或多个目的地。目的地可以包括电子邮件地址、移动设备的电话号码或其中可以发送信息的任何其它位置。

[0110] 在步骤510处，可以将临时访问信息发送到目的地。目的地可以是基于验证请求中的用户标识信息识别出的目的地。可以发送临时访问信息以供用户认证计算系统。临时访问信息可以是用户用来确认临时访问信息的发送者的一次性密码(OTP)。临时访问信息可以使得用户能够检验访问管理系统的计算系统实际上是访问管理系统的真正计算系统。

[0111] 为了保护对由访问管理系统管理的用户账户的未授权访问，访问管理系统可以在与客户端设备不同的目的地处与用户通信。目的地可以是来自请求访问管理系统的验证的客户端设备的带外或信道外。目的地可以位于用户可访问或者可以对于用户可访问(例如，存储器中的位置或在远程计算系统处可访问的位置)的设备上。可以选择目的地，使得其对于意图欺骗性地获得对用户账户访问的未授权系统是未知的。例如，目的地是与发送验证请求的客户端设备(例如，终端)不同的客户端设备(例如，移动设备)。在另一个示例中，目的地是可以向其发送包括临时访问信息的电子邮件消息的电子邮件地址。在一些实施例中，目的地是从其接收到验证请求的同一客户端设备。

[0112] 在步骤512处，可以从客户端设备(例如，发送验证请求的客户端设备)接收响应。响应可以包括发送到目的地的临时访问信息。用户可以从目的地获得临时访问信息。在一些实施例中，可以在客户端设备处呈现诸如参考图7所示的GUI，以接收由用户从目的地获得的临时访问信息。临时访问信息可以被包括在从GUI接收到的响应中。

[0113] 在步骤514处，可以检验在步骤512处的响应中接收到的临时访问信息。访问管理系统可以确定从客户端设备接收到的临时访问信息是否与发送到目的地的临时访问信息相同或匹配。在一些实施例中，临时访问信息可以是有限的或临时的，使得它与一个或多个约束(例如，时间段)相关联。临时访问信息虽然由目的地接收，但当(一个或多个)约束条件不满足时可能无效。检验临时访问信息可以包括确定用于临时访问信息的(一个或多个)约束是否已经被满足。

[0114] 在步骤516处，关于发送验证请求的客户端设备的用户的个人信息可以被发送到客户端设备。在检验临时访问信息满足约束之后，可以将个人信息发送到客户端设备。作为访问管理系统的验证的一部分，访问管理系统可以提供关于用户的个人信息以使得用户能够在用户向访问管理系统提供他/她的凭证之前检验其真实性。个人信息可以包括其它计算系统(例如，被设计为欺骗性地获得对用户账户的访问的网络钓鱼或黑客计算系统)不可访问的当前信息。个人信息可以由用户授权访问管理系统访问的一个或多个源供给。个人信息的示例可以包括财务信息(例如，最近交易、最近账户余额等)或其它私有或机密信息。

个人信息可以包括最近已被更新的信息，使得未授权访问的机会可能性不大。

[0115] 当客户端设备接收到个人信息时，客户端设备可以在GUI中显示个人信息，诸如参考图8描述的示例。通过GUI，用户可以检验个人信息以确认其真实性。GUI可以包括一个或多个交互元素，以接收与在步骤506处与验证请求一起接收到的用户标识信息相关联的用户的个人信息和凭证信息(例如，密码)的确认。

[0116] 在步骤518处，可以从请求访问管理系统的验证的客户端设备接收响应。响应于经由GUI接收到的指示检验在步骤516处发送的个人信息准确的输入，可以从客户端设备接收响应。响应可以包括确认个人信息的用户的凭证数据。凭证数据可以包括用于访问与在步骤506处接收到的用户标识信息相关联的账户的凭证信息(例如，密码)。

[0117] 在步骤518处发送响应的用户可以被认证以确定从客户端设备对资源的访问。可以基于在步骤518处接收到的凭证数据来认证用户。可以将凭证数据与存储的用于用户的用户标识信息的凭证信息进行比较，以确定它们是否匹配。在步骤520处，在确定凭证数据与存储的凭证信息匹配之后，可以认证用户访问资源。在用户认证之后，可以在客户端设备处为用户建立会话以访问资源。在一些实施例中，可以基于在步骤518处接收到的响应中的接收确认来进一步认证用户。基于确定用户被认证从客户端设备访问资源，可以向用户授权访问。该流程图在步骤522处结束。

[0118] 图6-9图示出根据实施例的用于使得用户能够验证访问管理系统的真实性的界面(例如，GUI)。图6-9中的每个GUI可以显示在应用中，例如图1的应用108中。GUI 600可以由管理对一个或多个资源的访问的访问管理应用显示。GUI 600可以由客户端设备生成、可以从生成GUI的访问管理系统接收、或者其组合。GUI 600可以由访问管理系统经由网络提供作为服务(例如，云服务)或网络可访问应用的一部分。在至少一个示例中，访问管理系统的操作员可以操作客户端设备以与GUI 600进行交互。

[0119] 现在转到图6，描绘了使得用户能够输入凭证信息以建立会话(例如，SSO会话)来访问一个或多个资源的GUI 600。GUI 600可以包括一个或多个交互元素以使得用户能够获得对提供会话的账户的访问。例如，GUI 600可以包括交互元素610以接收诸如用户标识信息(例如，用户名)的凭证信息。GUI 600可以包括接收输入以启动用于用户的认证的访问处理(例如，登录处理)的交互元素630。访问处理可以使得用户能够访问由访问管理系统管理的账户。通过启动访问处理，可以显示关于图9描述的GUI以接收输入，例如，凭证信息(例如，密码)，以确定与用户标识信息相关联的用户的访问。

[0120] 在一些实施例中，GUI 600可以包括交互元素620，该交互元素620接收输入以启动确认请求来确定经由GUI 600请求凭证信息的计算系统的真实性。通过启动确认请求，可以使得用户能够确定请求凭证信息的计算系统是否实际上是管理对与凭证信息相关联的账户的访问的真正(例如，非欺诈性)系统。

[0121] 图7中，描绘了使得用户能够输入临时访问信息(例如，一次性密码)的GUI 700。如上所述，临时访问信息可以由客户端设备从访问管理系统的计算系统接收作为认证处理的一部分。访问管理系统可以通过向目的地(例如，与请求访问管理系统的验证的客户端设备不同的设备)发送临时访问信息来建立其真实性。作为验证访问管理系统的处理的一部分，访问管理系统可以向客户端设备(例如，启动验证请求的客户端设备)发送请求以接收发送到目的地的临时访问信息。在一些实施例中，客户端设备可以显示经由交互元素710接收临

时访问信息的GUI 700。GUI 700可以包括交互元素720，该交互元素720接收向访问管理系统发送(例如，提交)临时访问信息的输入。临时访问信息可以被提交给访问管理系统。访问管理系统可以确认用户对临时访问信息的检验。访问管理系统可以检验临时访问信息以确定它是否与发送到目的地的临时访问信息匹配。

[0122] 在图8中，示出了使得用户能够确定访问管理系统的真实性的GUI 800。GUI 800可以显示关于请求访问管理系统的验证的用户的个人信息。如上所述，访问管理系统可以将关于用户的个人信息发送到由请求访问管理系统的验证的用户操作的客户端设备。个人信息可以在检验从用户接收到的临时访问信息之后发送给用户。在一些实施例中，可以将个人信息发送给启动请求以确定访问管理系统的真实性的客户端设备。

[0123] 客户端设备可以显示GUI 800以提供用于由操作客户端设备的用户检验的个人信息。个人信息可以作为用于验证访问管理系统的真实性的处理的一部分来提供。用户可以查看由GUI 800显示的个人信息以确定它是否准确。GUI 800可以包括一个或多个交互元素以接收指示个人信息是否准确的输入。(一个或多个)交互元素可以使得用户能够向访问管理系统提交请求来确认个人信息的准确性。在一些实施例中，GUI 800中的(一个或多个)交互元素可以接收输入以发送访问为其显示个人信息的用户的账户的访问请求(例如，登录请求)。例如，GUI 800可以包括接收用于请求访问账户的输入的交互元素820。在经由交互元素820接收到输入之后，访问请求可以被提交给访问管理系统。GUI 800可以包括交互元素810以接收访问为其显示个人信息的用户的账户的访问信息(例如，密码)。访问信息可以与在参考图6描述的GUI中接收到的用户标识信息对应。可以将访问信息与访问请求一起提交给访问管理系统。访问管理系统可以基于检验使用GUI 800提交的访问信息来确定对账户的访问。

[0124] 图9描绘了使得用户能够提供访问信息(例如，密码)以请求访问与用户相关联的账户的GUI 900。账户可以由与账户相关联的用户标识来识别。用户标识信息可以在不同的GUI中提供，例如，参考图6描述的GUI 600。GUI 900可以在通过与图6的交互元素630交互而启动访问处理时显示。GUI 900可以包括交互元素910以接收账户的凭证信息。交互元素920可以是交互式的，以基于凭证信息确定登录处理。在一些实施例中，当用户决定不验证访问管理系统的真实性时，可以显示GUI 900。在一些实施例中，可以组合GUI 900和GUI 600以减少用户为访问处理提供凭证信息的步骤数量。

[0125] 图10绘出了用于实现实施例的分布式系统1000的简化图。在所示的实施例中，分布式系统1000包括一个或多个客户端计算设备1002、1004、1006和1008，这些客户端计算设备被配置为通过一个或多个网络1010执行和操作客户端应用，诸如web浏览器、专有客户端(例如Oracle Forms)等。服务器1012可以经由网络1010与远程客户端计算设备1002、1004、1006和1008通信地耦合。

[0126] 在各种实施例中，服务器1012可以适于运行一个或多个服务或软件应用。在某些实施例中，服务器1012还可以提供其它服务，或者软件应用可以包括非虚拟和虚拟环境。在一些实施例中，这些服务可以作为基于web的或云服务或者在软件即服务(SaaS)模型下提供给客户端计算设备1002、1004、1006和/或1008的用户。操作客户端计算设备1002、1004、1006和/或1008的用户可以进而利用一个或多个客户端应用与服务器1012交互，以利用由这些部件提供的服务。

[0127] 在图10所绘出的配置中，系统1000的软件部件1018、1020和1022被示为在服务器1012上实现。在其它实施例中，系统1000的一个或多个部件和/或由这些部件提供的服务也可以由客户端计算设备1002、1004、1006和/或1008中的一个或多个实现。操作客户端计算设备的用户然后可以利用一个或多个客户端应用来使用由这些部件提供的服务。这些部件可以用硬件、固件、软件或其组合实现。应当理解，各种不同的系统配置是可能的，其可以与分布式系统1000不同。因此，图10中所示的实施例是用于实现实施例系统的分布式系统的一个示例，并且不旨在进行限制。

[0128] 客户端计算设备1002、1004、1006和/或1008可以包括各种类型的计算系统。例如，客户端计算设备可以包括便携式手持设备(例如，**iPhone®**、蜂窝电话、**iPad®**、计算平板、个人数字助理(PDA))或可穿戴设备(例如，Google**Glass®**头戴式显示器)，其运行诸如Microsoft Windows**Mobile®**之类的软件和/或诸如iOS、Windows Phone、Android、BlackBerry 10，Palm OS之类的各种移动操作系统。设备可以支持各种应用，诸如各种互联网相关的应用、电子邮件、短消息服务(SMS)应用，并且可以使用各种其它通信协议。客户端计算设备还可以包括通用个人计算机，作为示例，运行各种版本的Microsoft **Windows®**、Apple **Macintosh®**和/或Linux操作系统的个人计算机和/或膝上型计算机。客户端计算设备可以是运行任何各种商用的**UNIX®**或类UNIX操作系统(包括但不限于诸如像Google Chrome OS的各种GNU/Linux操作系统)的工作站计算机。客户端计算设备还可以包括能够提供(一个或多个)网络1010通信的电子设备，诸如瘦客户端计算机、启用互联网的游戏系统(例如，具有或不具有**Kinect®**手势输入设备的Microsoft **Xbox®**游戏控制台)和/或个人消息传送设备。

[0129] 虽然图10中的分布式系统1000被示为具有四个客户端计算设备，但是可以支持任何数量的客户端计算设备。其它设备，诸如具有传感器的设备等，可以与服务器1012交互。

[0130] 分布式系统1000中的(一个或多个)网络1010可以是对本领域技术人员熟悉的可以利用任何各种可用协议支持数据通信的任何类型的网络，其中各种协议包括但不限于TCP/IP(传输控制协议/互联网协议)、SNA(系统网络体系架构)、IPX(互联网分组交换)、AppleTalk等。仅仅作为示例，(一个或多个)网络1010可以是局域网(LAN)、基于以太网的网络、令牌环、广域网、互联网、虚拟网络、虚拟专用网络(VPN)、内联网、外联网、公共交换电话网络(PSTN)、红外网络、无线网络(例如，在任何电气和电子协会(IEEE)802.11协议套件、**Bluetooth®**、和/或任何其它无线协议下操作的网络)和/或这些和/或其它网络的任意组合。

[0131] 服务器1012可以由一个或多个通用计算机、专用服务器计算机(作为示例，包括PC(个人计算机)服务器、**UNIX®**服务器、中档服务器、大型计算机、机架安装的服务器等)、服务器场、服务器集群或任何其它适当的布置和/或组合组成。服务器1012可以包括运行虚拟操作系统的一个或多个虚拟机，或涉及虚拟化的其它计算体系架构。一个或多个灵活的逻辑存储设备池可以被虚拟化，以维护用于服务器的虚拟存储设备。虚拟网络可以由服务器1012利用软件定义的联网来控制。在各种实施例中，服务器1012可以适于运行在前述公开内容中描述的一个或多个服务或软件应用。例如，服务器1012可以与根据本公开的实施例的用于如上所述执行处理的服务器对应。

[0132] 服务器1012可以运行包括以上讨论的任何操作系统的操作系统，以及任何商用的服务器操作系统。服务器1012还可以运行任何各种附加的服务器应用和/或中间层应用，包括HTTP(超文本传输协议)服务器、FTP(文件传输协议)服务器、CGI(公共网关接口)服务器、JAVA®服务器、数据库服务器等。示例性数据库服务器包括但不限于可从Oracle、Microsoft、Sybase、IBM(国际商业机器)等商业获得的数据库服务器。

[0133] 在一些实现中，服务器1012可以包括一个或多个应用，以分析和整合从客户端计算设备1002、1004、1006和1008的用户接收到的数据馈送和/或事件更新。作为示例，数据馈送和/或事件更新可以包括但不限于从一个或多个第三方信息源和持续数据流接收到的Twitter®馈送、Facebook®更新或实时更新，其可以包括与传感器数据应用、金融报价机、网络性能测量工具(例如，网络监视和流量管理应用)、点击流分析工具、汽车流量监视等相关的实时事件。服务器1012还可以包括经由客户端计算设备1002、1004、1006和1008的一个或多个显示设备显示数据馈送和/或实时事件的一个或多个应用。

[0134] 分布式系统1000也可以包括一个或多个数据库1014和1016。这些数据库可以提供用于存储信息的机制，诸如用户交互信息、使用模式信息、适应规则信息以及由本发明的实施例使用的其它信息。数据库1014和1016可以驻留在各种位置中。作为示例，数据库1014和1016中的一个或多个可以驻留在服务器1012本地(和/或驻留在其中)的非瞬态存储介质上。可替代地，数据库1014和1016可以远离服务器1012，并且经由基于网络的或专用的连接与服务器1012通信。在一组实施例中，数据库1014和1016可以驻留在存储区域网络(SAN)中。类似地，用于执行服务器1012所具有的功能的任何必要的文件可以适当地在服务器1012本地存储和/或远程存储。在一组实施例中，数据库1014和1016可以包括适于响应于SQL格式的命令存储、更新和检索数据的关系数据库，诸如由Oracle提供的数据库。

[0135] 在一些实施例中，云环境可以提供一个或多个服务。图11是根据本公开内容的实施例、其中服务可以被提供为云服务的系统环境1100的一个或多个部件的简化框图。在图11所示的实施例中，系统环境1100包括可以被用户用来与提供云服务的云基础设施系统1102交互的一个或多个客户端计算设备1104、1106和1108。云基础设施系统1102可以包括一个或多个计算机和/或服务器，其可以包括以上针对服务器1012所描述的那些。

[0136] 应当认识到的是，图11中所绘出的云基础设施系统1102可以具有除所绘出的那些之外的其它部件。另外，图11中所示的实施例仅仅是可以结合本发明的实施例的云基础设施系统的一个示例。在一些其它实施例中，云基础设施系统1102可以具有比图中所示出的更多或更少的部件、可以合并两个或更多个部件、或者可以具有不同的部件配置或布置。

[0137] 客户端计算设备1104、1106和1108可以是与以上针对客户端计算设备1002、1004、1006和1008描述的那些设备类似的设备。客户端计算设备1104、1106和1108可以被配置为操作客户端应用，诸如web浏览器、专有客户端应用(例如，Oracle Forms)或可以被客户端计算设备的用户使用以与云基础设施系统1102交互来使用由云基础设施系统1102提供的服务的一些其它应用。虽然示例性系统环境1100被示为具有三个客户端计算设备，但是可以支持任何数量的客户端计算设备。诸如具有传感器的设备等的其它设备可以与云基础设施系统1102交互。

[0138] (一个或多个)网络1110可以促进客户端计算设备1104、1106和1108与云基础设施系统1102之间的通信和数据交换。每个网络可以是对本领域技术人员熟悉的可以利用任何

各种商用的协议支持数据通信的任何类型的网络，其中协议包括以上针对(一个或多个)网络1010所描述的协议。

[0139] 在某些实施例中，由云基础设施系统1102提供的服务可以包括按需对云基础设施系统的用户可用的服务的主机。还可以提供各种其它服务，包括但不限于在线数据存储和备份解决方案、基于Web的电子邮件服务、托管的办公套件和文档协作服务、数据库处理、受管理的技术支持服务等。由云基础设施系统提供的服务可以动态扩展，以满足其用户的需求。

[0140] 在某些实施例中，由云基础设施系统1102提供的服务的具体实例化在本文中可以被称为“服务实例”。一般而言，经由通信网络(诸如互联网)从云服务提供者的系统使得对用户可用的任何服务被称为“云服务”。通常，在公共云环境中，构成云服务提供者的系统的服务器和系统与消费者自己的本地服务器和系统不同。例如，云服务提供者的系统可以托管应用，并且用户可以经由诸如互联网的通信网络按需订购和使用应用。

[0141] 在一些示例中，计算机网络云基础设施中的服务可以包括对存储装置、托管的数据库、托管的web服务器、软件应用或者由云供应商向用户提供的其它服务的受保护的计算机网络访问，或者如本领域中另外已知的。例如，服务可以包括通过互联网对云上的远程存储的受密码保护的访问。作为另一个示例，服务可以包括基于web服务的托管的关系数据库和脚本语言中间件引擎，用于由联网的开发人员私人使用。作为另一个示例，服务可以包括对在云供应商的网站上托管的电子邮件软件应用的访问。

[0142] 在某些实施例中，云基础设施系统1102可以包括以自助服务、基于订阅、弹性可扩展、可靠、高度可用和安全的方式交付给消费者的应用套件、中间件和数据库服务产品。这种云基础设施系统的示例是由本受让人提供的Oracle Public Cloud(Oracle公共云)。

[0143] 云基础设施系统1102还可以提供与“大数据”相关的计算和分析服务。术语“大数据”一般用来指可由分析员和研究者存储和操纵以可视化大量数据、检测趋势和/或以其它方式与数据交互的极大数据集。这种大数据和相关应用可以在许多级别和不同规模上由基础设施系统托管和/或操纵。并行链接的数十个、数百个或数千个处理器可以作用于这种数据，以便呈现其或者模拟对数据或其所表示的内容的外力。这些数据集可以涉及结构化数据，诸如在数据库中组织或以其它方式根据结构化模型组织的数据，和/或者非结构化数据(例如，电子邮件、图像、数据blob(二进制大对象)、网页、复杂事件处理)。通过利用实施例相对快速地将更多(或更少)的计算资源聚焦在目标上的能力，云基础设施系统可以更好地用于基于来自企业、政府机构、研究组织、私人个人、一群志同道合的个人或组织或其它实体的需求在大数据集上执行任务。

[0144] 在各种实施例中，云基础设施系统1102可以适于自动地供应、管理和跟踪消费者对由云基础设施系统1102提供的服务的订阅。云基础设施系统1102可以经由不同的部署模型提供云服务。例如，服务可以在公共云模型下提供，其中云基础设施系统1102由销售云服务的组织拥有(例如，由Oracle公司拥有)并且使服务对一般公众或不同的工业企业可用。作为另一个示例，服务可以在私有云模型下提供，其中云基础设施系统1102仅针对单个组织操作，并且可以为组织内的一个或多个实体提供服务。云服务还可以在社区云模型下提供，其中云基础设施系统1102和由云基础设施系统1102提供的服务由相关社区中的若干个组织共享。云服务还可以在混合云模型下提供，混合云模型是两个或更多个不同模型的组

合。

[0145] 在一些实施例中，由云基础设施系统1102提供的服务可以包括在软件即服务(SaaS)类别、平台即服务(PaaS)类别、基础设施即服务(IaaS)类别、或包括混合服务的服务的其它类别下提供的一个或多个服务。消费者经由订阅订单可以订购由云基础设施系统1102提供的一个或多个服务。云基础设施系统1102然后执行处理，以提供消费者的订阅订单中的服务。

[0146] 在一些实施例中，由云基础设施系统1102提供的服务可以包括但不限于应用服务、平台服务和基础设施服务。在一些示例中，应用服务可以由云基础设施系统经由SaaS平台提供。SaaS平台可以被配置为提供属于SaaS类别的云服务。例如，SaaS平台可以提供在集成的开发和部署平台上构建和交付点播应用套件的能力。SaaS平台可以管理和控制用于提供SaaS服务的底层软件和基础设施。通过利用由SaaS平台提供的服务，消费者可以利用在云基础设施系统上执行的应用。消费者可以获取应用服务，而无需消费者单独购买许可证和支持。可以提供各种不同的SaaS服务。示例包括但不限于为大型组织提供用于销售绩效管理、企业集成和业务灵活性的解决方案的服务。

[0147] 在一些实施例中，平台服务可以由云基础设施系统1102经由PaaS平台提供。PaaS平台可以被配置为提供属于PaaS类别的云服务。平台服务的示例可以包括但不限于使组织(诸如Oracle)能够在共享的共同体系架构上整合现有应用的服务，以及利用由平台提供的共享服务构建新应用的能力。PaaS平台可以管理和控制用于提供PaaS服务的底层软件和基础设施。消费者可以获取由云基础设施系统1102提供的PaaS服务，而无需消费者购买单独的许可证和支持。平台服务的示例包括但不限于Oracle Java云服务(JCS)、Oracle数据库云服务(DBCS)以及其它。

[0148] 通过利用由PaaS平台提供的服务，消费者可以采用由云基础设施系统支持的编程语言和工具，并且还控制所部署的服务。在一些实施例中，由云基础设施系统提供的平台服务可以包括数据库云服务、中间件云服务(例如，Oracle Fusion Middleware服务)和Java云服务。在一个实施例中，数据库云服务可以支持共享服务部署模型，其使得组织能够汇集数据库资源并且以数据库云的形式向消费者提供数据库即服务。中间件云服务可以为消费者提供开发和部署各种业务应用的平台，以及Java云服务可以在云基础设施系统中为消费者提供部署Java应用的平台。

[0149] 可以由云基础设施系统中的IaaS平台提供各种不同的基础设施服务。基础设施服务促进底层计算资源(诸如存储装置、网络和其它基本计算资源)的管理和控制，以便消费者利用由SaaS平台和PaaS平台提供的服务。

[0150] 在某些实施例中，云基础设施系统1102还可以包括基础设施资源1130，用于提供用来向云基础设施系统的消费者提供各种服务的资源。在一个实施例中，基础设施资源1130可以包括执行由PaaS平台和SaaS平台提供的服务的硬件(诸如服务器、存储装置和联网资源)的预先集成和优化的组合，以及其它资源。

[0151] 在一些实施例中，云基础设施系统1102中的资源可以由多个用户共享并且按需动态地重新分配。此外，资源可以分配给在不同时区中的用户。例如，云基础设施系统1102可以使第一时区内的第一用户集合能够利用云基础设施系统的资源指定的小时数，然后使得能够将相同资源重新分配给位于不同时区中的另一用户集合，从而最大化资源的利用率。

[0152] 在某些实施例中，可以提供由云基础设施系统1102的不同部件或模块共享，以使得能够由云基础设施系统1102供应服务的多个内部共享服务1132。这些内部共享服务可以包括，但不限于，安全和身份服务、集成服务、企业储存库服务、企业管理器服务、病毒扫描和白名单服务、高可用性、备份和恢复服务、用于启用云支持的服务、电子邮件服务、通知服务、文件传输服务等。

[0153] 在某些实施例中，云基础设施系统1102可以在云基础设施系统中提供云服务(例如，SaaS、PaaS和IaaS服务)的综合管理。在一个实施例中，云管理功能可以包括用于供应、管理和跟踪由云基础设施系统1102等接收到的消费者的订阅的能力。

[0154] 在一个实施例中，如图11中所绘出的，云管理功能可以由诸如订单管理模块1120、订单编排模块1122、订单供应模块1124、订单管理和监视模块1126以及身份管理模块1128的一个或多个模块提供。这些模块可以包括或可以利用一个或多个计算机和/或服务器提供，该一个或多个计算机和/或服务器可以是通用计算机、专用服务器计算机、服务器场，服务器集群或任何其它适当的布置和/或组合。

[0155] 在示例性操作中，在1134，使用客户端设备(诸如客户端计算设备1104、1106或1108)的消费者可以通过请求由云基础设施系统1102提供的一个或多个服务并且对由云基础设施系统1102提供的一个或多个服务的订阅下订单来与云基础设施系统1102交互。在某些实施例中，消费者可以访问诸如云UI 1112、云UI 1114和/或云UI1116的云用户界面(UI)并经由这些UI下订阅订单。响应于消费者下订单而由云基础设施系统1102接收到的订单信息可以包括识别消费者和消费者打算订阅的由云基础设施系统1102提供的一个或多个服务的信息。

[0156] 在步骤1136处，从消费者接收到的订单信息可以存储在订单数据库1118中。如果这是新的订单，则可以为该订单创建新的记录。在一个实施例中，订单数据库1118可以是由云基础设施系统1118操作以及与其它系统元素结合操作的若干数据库当中的一个。

[0157] 在步骤1138处，订单信息可以被转发到订单管理模块1120，订单管理模块1120可以被配置为执行与订单相关的计费和记帐功能，诸如检验订单，并且在通过检验之后，预订订单。

[0158] 在步骤1140处，关于订单的信息可以被传送到订单编排模块1122，订单编排模块1122被配置为编排用于由消费者下的订单的服务和资源的供应。在一些情况下，订单编排模块1122可以使用订单供应模块1124的服务用于供应。在某些实施例中，订单编排模块1122使得能够管理与每个订单相关联的业务过程，并且应用业务逻辑来确定订单是否应当继续供应。

[0159] 如图11中绘出的实施例所示，在1142处，在接收到新订阅的订单时，订单编排模块1122向订单供应模块1124发送分配资源和配置履行订购订单所需的资源的请求。订单供应模块1124使得能够为由消费者订购的服务分配资源。订单供应模块1124提供由云基础设施系统1100提供的云服务和用来供应用于提供所请求的服务的资源的物理实现层之间的抽象级别。这使得订单编排模块1122能够与实现细节隔离，诸如服务和资源是否实际上实时供应，或者预先供应并且仅在请求时才进行分配/指定。

[0160] 在步骤1144处，一旦供应了服务和资源，就可以向订阅的消费者发送指示所请求的服务现在已准备好用于使用的通知。在一些情况下，可以向消费者发送使得消费者能够

开始使用所请求的服务的信息(例如,链接)。

[0161] 在步骤1146处,可以由订单管理和监视模块1126来管理和跟踪消费者的订阅订单。在一些情况下,订单管理和监视模块1126可以被配置为收集关于消费者使用所订阅的服务的使用统计。例如,可以针对所使用的存储量、所传送的数据量、用户的数量以及系统启动时间和系统停机时间的量等来收集统计数据。

[0162] 在某些实施例中,云基础设施系统1100可以包括身份管理模块1128,其被配置为提供身份服务,诸如云基础设施系统1100中的访问管理和授权服务。在一些实施例中,身份管理模块1128可以控制关于希望利用由云基础设施系统1102提供的服务的消费者的信息。这种信息可以包括认证这些消费者的身份的信息和描述那些消费者被授权相对于各种系统资源(例如,文件、目录、应用、通信端口、存储器段等)执行的动作的信息。身份管理模块1128还可以包括关于每个消费者的描述性信息以及关于如何和由谁来访问和修改描述性信息的管理。

[0163] 图12图示了可以被用来实现本公开的实施例的示例性计算机系统1200。在一些实施例中,计算机系统1200可以被用来实现上述任何各种服务器和计算机系统。如图12所示,计算机系统1200包括各种子系统,包括经由总线子系统1202与多个外围子系统通信的处理单元1204。这些外围子系统可以包括处理加速单元1206、I/O子系统1208、存储子系统1218和通信子系统1224。存储子系统1218可以包括有形的计算机可读存储介质1222和系统存储器1210。

[0164] 总线子系统1202提供用于使计算机系统1200的各种部件和子系统按照期望彼此通信的机制。虽然总线子系统1202被示意性地示为单条总线,但是总线子系统的可替代实施例可以利用多条总线。总线子系统1202可以是若干种类型的总线结构中的任何一种,包括存储器总线或存储器控制器、外围总线和利用任何各种总线体系架构的局部总线。例如,此类体系架构可以包括工业标准体系架构(ISA)总线、微通道体系架构(MCA)总线、增强型ISA(EISA)总线、视频电子标准协会(VESA)局部总线和外围部件互连(PCI)总线,其可以实现为根据IEEE P1386.1标准制造的夹层(Mezzanine)总线,等等。

[0165] 处理子系统1204控制计算机系统1200的操作并且可以包括一个或多个处理单元1232、1234等。处理单元可以包括一个或多个处理器,其中包括单核或多核处理器、处理器的一个或多个核、或其组合。在一些实施例中,处理子系统1204可以包括一个或多个专用协处理器,诸如图形处理器、数字信号处理器(DSP)等。在一些实施例中,处理子系统1204的处理单元中的一些或全部可以利用定制电路来实现,诸如专用集成电路(ASIC)或现场可编程门阵列(FPGA)。

[0166] 在一些实施例中,处理子系统1204中的处理单元可以执行存储在系统存储器1210中或计算机可读存储介质1222上的指令。在各种实施例中,处理单元可以执行各种程序或代码指令,并且可以维护多个并发执行的程序或进程。在任何给定的时间,要执行的程序代码中的一些或全部可以驻留在系统存储器1210中和/或计算机可读存储介质1222上,潜在地包括在一个或多个存储设备上。通过适当的编程,处理子系统1204可以提供各种功能。

[0167] 在某些实施例中,可以提供处理加速单元1206,用于执行定制的处理或用于卸载由处理子系统1204执行的一些处理,以便加速由计算机系统1200执行的整体处理。

[0168] I/O子系统1208可以包括用于向计算机系统1200输入信息和/或用于从或经由计

算机系统1200输出信息的设备和机制。一般而言，术语“输入设备”的使用旨在包括用于向计算机系统1200输入信息的所有可能类型的设备和机制。用户接口输入设备可以包括，例如，键盘、诸如鼠标或轨迹球的指示设备、结合到显示器中的触摸板或触摸屏、滚轮、点拨轮、拨盘、按钮、开关、键板、具有语音命令识别系统的音频输入设备、麦克风以及其它类型的输入设备。用户接口输入设备也可以包括使用户能够控制输入设备并与其交互的诸如Microsoft **Kinect®**运动传感器的运动感测和/或姿势识别设备、Microsoft **Xbox®**360游戏控制器、提供用于接收利用姿势和口语命令的输入的接口的设备。用户接口输入设备也可以包括眼睛姿势识别设备，诸如从用户检测眼睛活动(例如，当拍摄图片和/或进行菜单选择时的“眨眼”)并将眼睛姿势转换为到输入设备(例如，Google **Glass®**)中的输入的Google **Glass®**眨眼检测器。此外，用户接口输入设备可以包括使用户能够通过语音命令与语音识别系统(例如，**Siri®**导航器)交互的语音识别感测设备。

[0169] 用户接口输入设备的其它示例包括但不限于，三维(3D)鼠标、操纵杆或指示杆、游戏板和图形平板、以及音频/视频设备，诸如扬声器、数字相机、数字摄像机、便携式媒体播放器、网络摄像机、图像扫描仪、指纹扫描仪、条形码读取器3D扫描仪、3D打印机、激光测距仪、以及眼睛注视跟踪设备。此外，用户接口输入设备可以包括，例如，医疗成像输入设备，诸如计算机断层摄影、磁共振成像、位置发射断层摄影、医疗超声检查设备。用户接口输入设备也可以包括，例如，音频输入设备，诸如MIDI键盘、数字乐器等。

[0170] 用户接口输出设备可以包括显示子系统、指示器灯或诸如音频输出设备的非可视显示器等。显示子系统可以是阴极射线管(CRT)、诸如利用液晶显示器(LCD)或等离子体显示器的平板设备、投影设备、触摸屏等。一般而言，术语“输出设备”的使用旨在包括用于从计算机系统1200向用户或其它计算机输出信息的所有可能类型的设备和机制。例如，用户接口输出设备可以包括但不限于，可视地传达文本、图形和音频/视频信息的各种显示设备，诸如监视器、打印机、扬声器、耳机、汽车导航系统、绘图仪、语音输出设备和调制解调器。

[0171] 存储子系统1218提供用于存储由计算机系统1200使用的信息的储存库或数据存储。存储子系统1218提供有形非瞬态计算机可读存储介质，用于存储提供一些实施例的功能的基本编程和数据结构。当由处理子系统1204执行时提供上述功能的软件(程序、代码模块、指令)可以存储在存储子系统1218中。软件可以由处理子系统1204的一个或多个处理单元执行。存储子系统1218也可以提供用于存储根据本发明使用的数据的储存库。

[0172] 存储子系统1218可以包括一个或多个非瞬态存储器设备，包括易失性和非易失性存储器设备。如图12所示，存储子系统1218包括系统存储器1210和计算机可读存储介质1222。系统存储器1210可以包括多个存储器，包括用于在程序执行期间存储指令和数据的易失性主随机存取存储器(RAM)和其中存储固定指令的非易失性只读存储器(ROM)或闪存存储器。在一些实现中，包含帮助在诸如启动期间在计算机系统1200内的元件之间传送信息的基本例程的基本输入/输出系统(BIOS)通常可以存储在ROM中。RAM通常包含当前由处理子系统1204操作和执行的数据和/或程序模块。在一些实现中，系统存储器1210可以包括多个不同类型的存储器，诸如静态随机存取存储器(SRAM)或动态随机存取存储器(DRAM)。

[0173] 作为示例而非限制，如在图12中所绘出的，系统存储器1210可以存储应用程序

1212,其可以包括客户端应用、Web浏览器、中间层应用、关系数据库管理系统(RDBMS)等、程序数据1214和操作系统1216。作为示例,操作系统1216可以包括各种版本的Microsoft **Windows®**、Apple **Macintosh®**和/或Linux操作系统、各种商用**UNIX®**或类UNIX操作系统(包括但不限于各种GNU/Linux操作系统、Google **Chrome®** OS等)和/或诸如iOS、**Windows®** Phone、**Android®** OS、**BlackBerry®** 8OS和**Palm®** OS操作系统的移动操作系统。

[0174] 计算机可读存储介质1222可以存储提供一些实施例的功能的编程和数据结构。当由处理子系统1204执行时使处理器提供上述功能的软件(程序、代码模块、指令)可以存储在存储子系统1218中。作为示例,计算机可读存储介质1222可以包括非易失性存储器,诸如硬盘驱动器、磁盘驱动器、诸如CD ROM、DVD、**Blu-Ray®** (蓝光)盘或其它光学介质的光盘驱动器。计算机可读存储介质1222可以包括但不限于,**Zip®**驱动器、闪存存储器卡、通用串行总线(USB)闪存驱动器、安全数字(SD)卡、DVD盘、数字视频带等。计算机可读存储介质1222也可以包括基于非易失性存储器的固态驱动器(SSD)(诸如基于闪存存储器的SSD、企业闪存驱动器、固态ROM等)、基于易失性存储器的SSD(诸如基于固态RAM、动态RAM、静态RAM、DRAM的SSD、磁阻RAM(MRAM)SSD),以及使用基于DRAM和基于闪存存储器的SSD的组合的混合SSD。计算机可读介质1222可以为计算机系统1200提供计算机可读指令、数据结构、程序模块和其它数据的存储。

[0175] 在某些实施例中,存储子系统1200也可以包括计算机可读存储介质读取器1220,其可以进一步连接到计算机可读存储介质1222。可选地,与系统存储器1210一起和组合,计算机可读存储介质1222可以全面地表示远程、本地、固定和/或可移动存储设备加上用于存储计算机可读信息的存储介质。

[0176] 在某些实施例中,计算机系统1200可以提供对执行一个或多个虚拟机的支持。计算机系统1200可以执行诸如管理程序的程序,以便促进虚拟机的配置和管理。每个虚拟机可以被分配存储器、计算(例如,处理器、内核)、I/O和联网资源。每个虚拟机通常运行其自己的操作系统,其可以与由计算机系统1200执行的其它虚拟机执行的操作系统相同或不同。相应地,多个操作系统可以潜在地由计算机系统1200并发地运行。每个虚拟机一般独立于其它虚拟机运行。

[0177] 通信子系统1224提供到其它计算机系统和网络的接口。通信子系统1224用作用于从计算机系统1200的其它系统接收数据和向其发送数据的接口。例如,通信子系统1224可以使计算机系统1200能够经由互联网建立到一个或多个客户端计算设备的通信信道,用于从客户端计算设备接收信息和发送信息到客户端计算设备。

[0178] 通信子系统1224可以支持有线和/或无线通信协议两者。例如,在某些实施例中,通信子系统1224可以包括用于(例如,使用蜂窝电话技术、高级数据网络技术(诸如3G、4G或EDGE(全球演进的增强数据速率)、WiFi(IEEE 802.11族标准)、或其它移动通信技术、或其任意组合)接入无线语音和/或数据网络的射频(RF)收发器部件、全球定位系统(GPS)接收器部件和/或其它部件。在一些实施例中,作为无线接口的附加或替代,通信子系统1224可以提供有线网络连接(例如,以太网)。

[0179] 通信子系统1224可以以各种形式接收和发送数据。例如,在一些实施例中,通信子

系统1224可以以结构化和/或非结构化的数据馈送1226、事件流1228、事件更新1230等形式接收输入通信。例如，通信子系统1224可以被配置为实时地从社交媒体网络的用户和/或诸如Twitter®馈送、Facebook®更新、诸如丰富站点摘要(RSS)馈送的web馈送的其它通信服务接收(或发送)数据馈送1226，和/或来自一个或多个第三方信息源的实时更新。

[0180] 在某些实施例中，通信子系统1224可以被配置为以连续数据流的形式接收本质上可能是连续的或无界的没有明确结束的数据，其中连续数据流可以包括实时事件的事件流1228和/或事件更新1230。生成连续数据的应用的示例可以包括例如传感器数据应用、金融报价机、网络性能测量工具(例如网络监视和流量管理应用)、点击流分析工具、汽车流量监视等。

[0181] 通信子系统1224也可以被配置为向一个或多个数据库输出结构化和/或非结构化的数据馈送1226、事件流1228、事件更新1230等，其中所述一个或多个数据库可以与耦合到计算机系统1200的一个或多个流数据源计算机通信。

[0182] 计算机系统1200可以是各种类型中的一种，包括手持便携式设备(例如，iPhone®蜂窝电话、iPad®计算平板、PDA)、可穿戴设备(例如，Google Glass®头戴式显示器)、个人计算机、工作站、大型机、信息站、服务器机架或任何其它数据处理系统。

[0183] 由于计算机和网络不断变化的性质，对图12中绘出的计算机系统1200的描述旨在仅仅作为具体示例。具有比图12中所绘出的系统更多或更少部件的许多其它配置是可能的。基于本文所提供的公开内容和教导，本领域普通技术人员将理解实现各种实施例的其它方式和/或方法。

[0184] 虽然已经描述了本发明的具体实施例，但是各种修改、更改、替代构造和等效物也包含在本发明的范围之内。修改包括所公开的特征的任何相关组合。本发明的实施例不限于在某些特定数据处理环境内的操作，而是可以在多个数据处理环境内自由操作。此外，虽然已利用特定系列的事务和步骤描述了本发明的实施例，但是，对本领域技术人员应当显而易见，本发明的范围不限于所描述系列的事务和步骤。上述实施例的各种特征和方面可以被单独或结合使用。

[0185] 另外，虽然已经利用硬件和软件的特定组合描述了本发明的实施例，但是应当认识到，硬件和软件的其它组合也在本发明的范围之内。本发明的实施例可以只用硬件、或只用软件、或利用其组合来实现。本文描述的各种过程可以在同一处理器或以任何组合的不同处理器上实现。相应地，在部件或模块被描述为被配置为执行某些操作的情况下，这种配置可以例如通过设计电子电路来执行操作、通过对可编程电子电路(诸如微处理器)进行编程来执行操作、或其任意组合来实现。进程可以利用各种技术来通信，包括但不限于用于进程间通信的常规技术，并且不同的进程对可以使用不同的技术，或者同一对进程可以在不同时间使用不同的技术。

[0186] 相应地，说明书和附图应当在说明性而不是限制性的意义上考虑。但是，将显而易见的是，在不背离权利要求中阐述的更广泛精神和范围的情况下，可以对其进行添加、减少、删除和其它修改和改变。因此，虽然已描述了具体发明实施例，但是这些实施例不旨在进行限制。各种修改和等效物都在以下权利要求的范围之内。

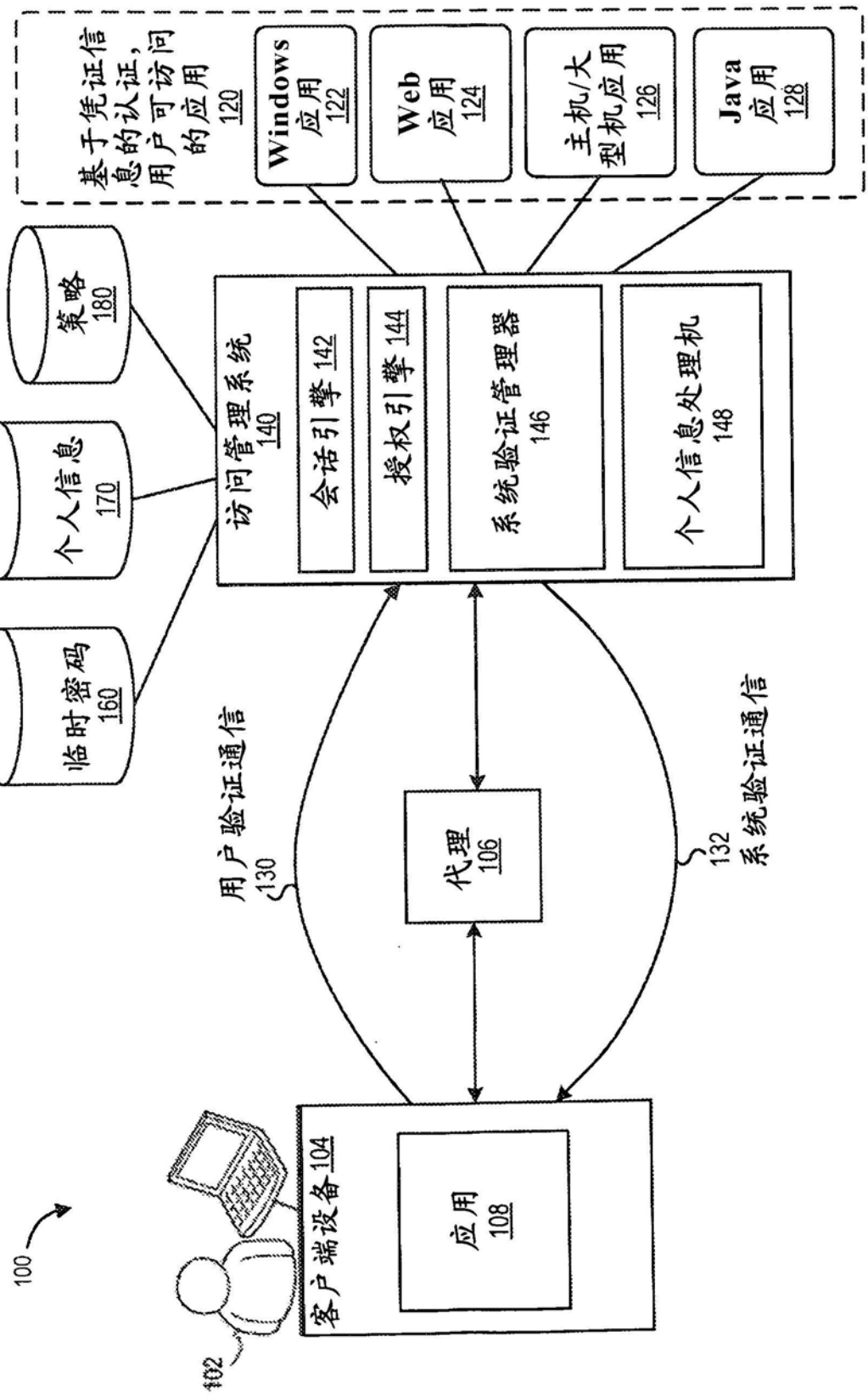

基于凭证信息的认证，用户可访问的应用 120
Windows 应用 122
Web 应用 124
主机/大型机应用 126
Java 应用 128
策略 180
个人信息 170
临时密码 160
访问管理系统 140
会话引擎 142
授权引擎 144
系统验证管理器 146
个人信息处理机 148
用户验证通信 130
代理 106
132 系统验证通信
客户端设备 104
应用 108
100
102

图1

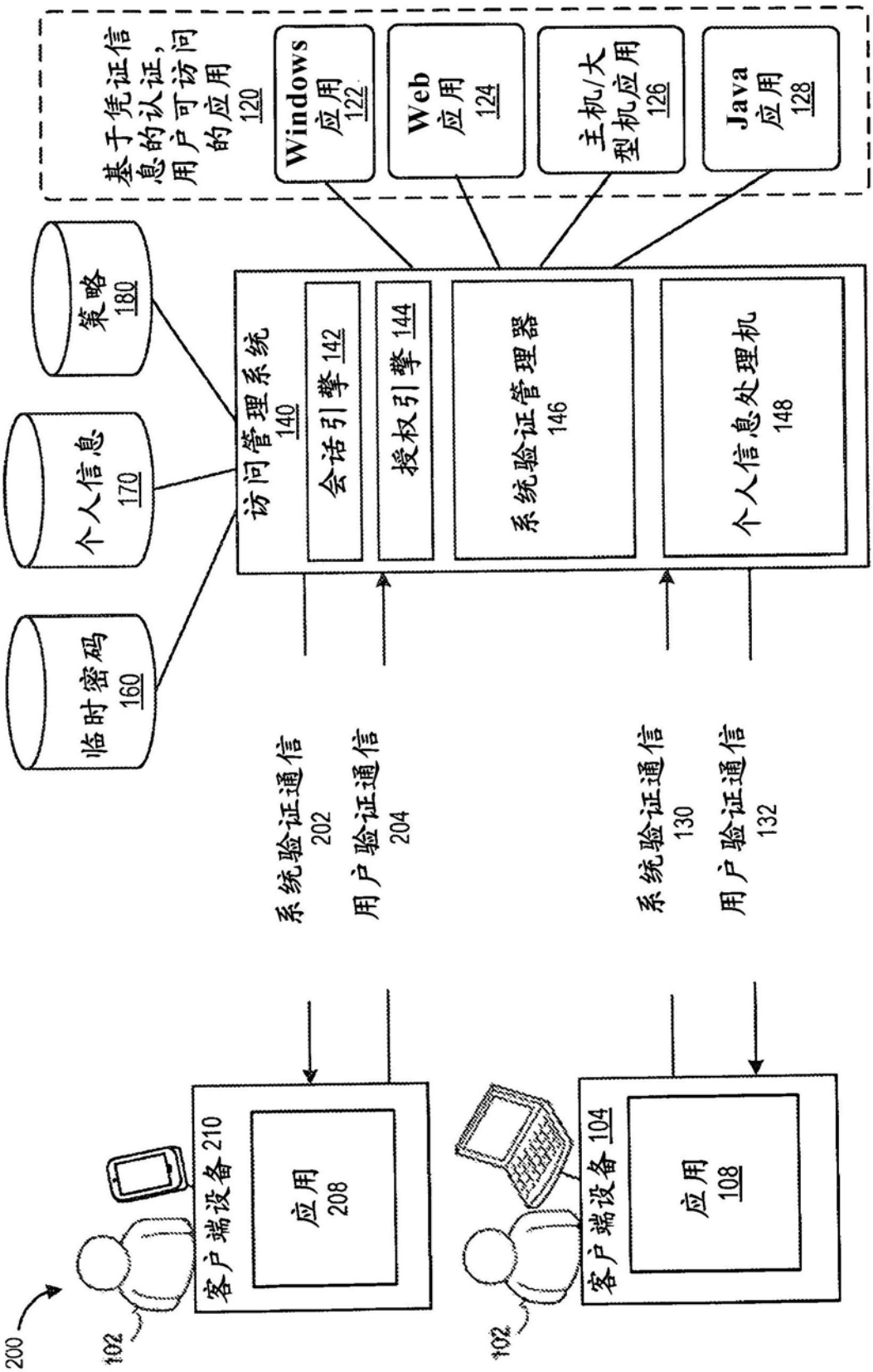

基于凭证信息的认证，用户可访问的应用 120
Windows 应用 122
Web 应用 124
主机/大型机应用 126
Java 应用 128
策略 180
个人信息 170
临时密码 160
访问管理系统 140
会话引擎 142
授权引擎 144
系统验证管理器 146
个人信息处理机 148
系统验证通信 202
用户验证通信 204
系统验证通信 130
用户验证通信 132
客户端设备 210
应用 208
客户端设备 104
应用 108
102
102
200

图2

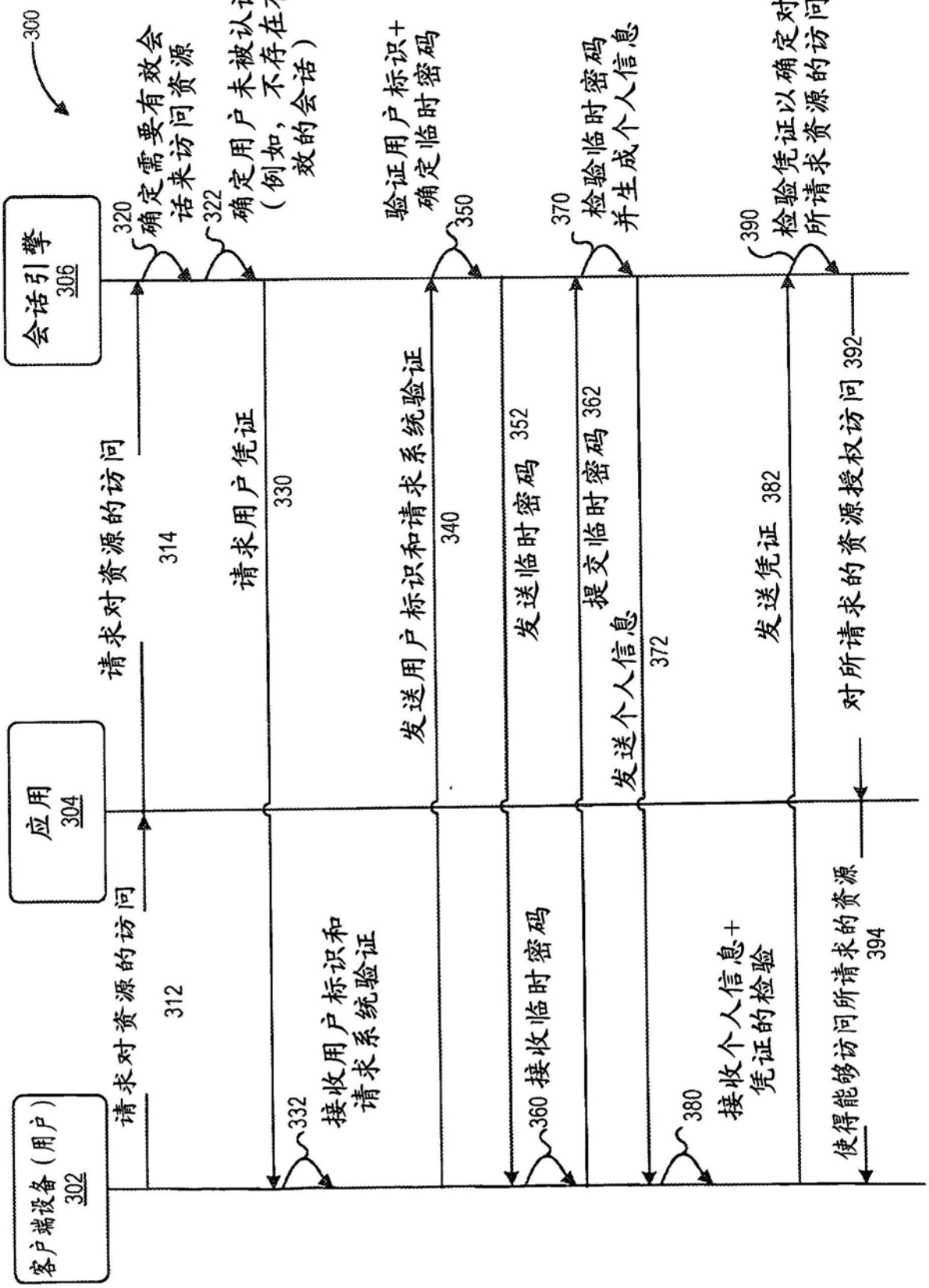

300
客户端设备（用户）
302
应用
304
会话引擎
306
请求对资源的访问
312
请求对资源的访问
314
320 确定需要有效会话来访问资源
322 确定用户未被认证（例如，不存在有效的会话）
请求用户凭证
330
332 接收用户标识和请求系统验证
发送用户标识和请求系统验证
340
验证用户标识+确定临时密码
350
发送临时密码 352
360 接收临时密码
提交临时密码 362
发送个人信息
372
检验临时密码并生成个人信息
370
380 接收个人信息+凭证的检验
发送凭证 382
检验凭证以确定对所请求资源的访问
390
对所请求的资源授权访问 392
使得能够访问所请求的资源
394

图3

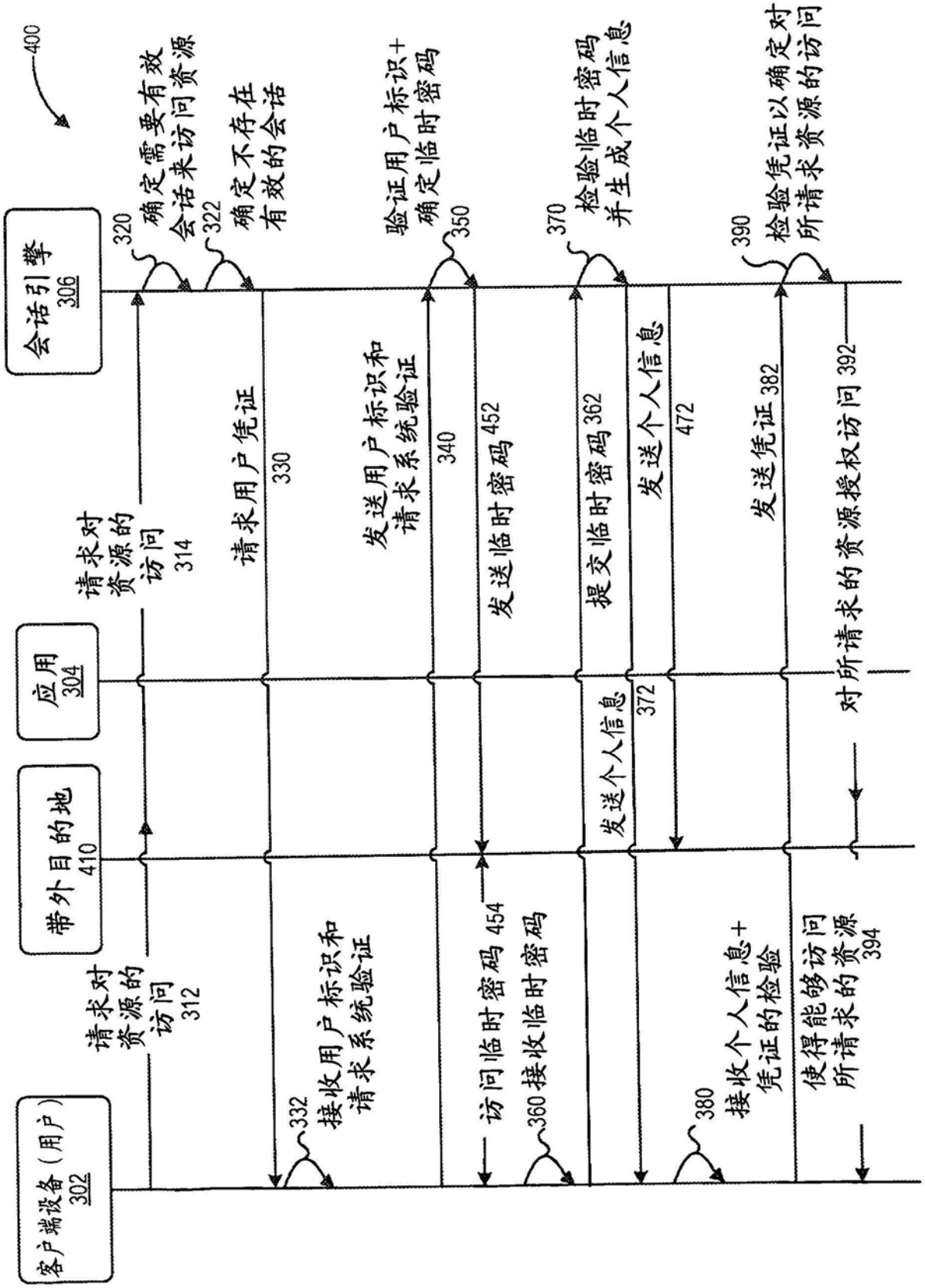

400
客户端设备（用户）
302
带外目的地
410
应用
304
会话引擎
306
请求对资源的访问
312
请求对资源的访问
314
320 确定需要有效会话来访问资源
322 确定不存在有效的会话
请求用户凭证
330
332 接收用户标识和请求系统验证
发送用户标识和请求系统验证
340
验证用户标识+确定临时密码
350
访问临时密码 454
360 接收临时密码
发送临时密码 452
提交临时密码 362
370 检验临时密码并生成个人信息
发送个人信息
372
发送个人信息
472
380 接收个人信息+凭证的检验
发送凭证 382
390 检验凭证以确定对所请求资源的访问
使得能够访问所请求的资源
394
对所请求的资源授权访问 392

图4

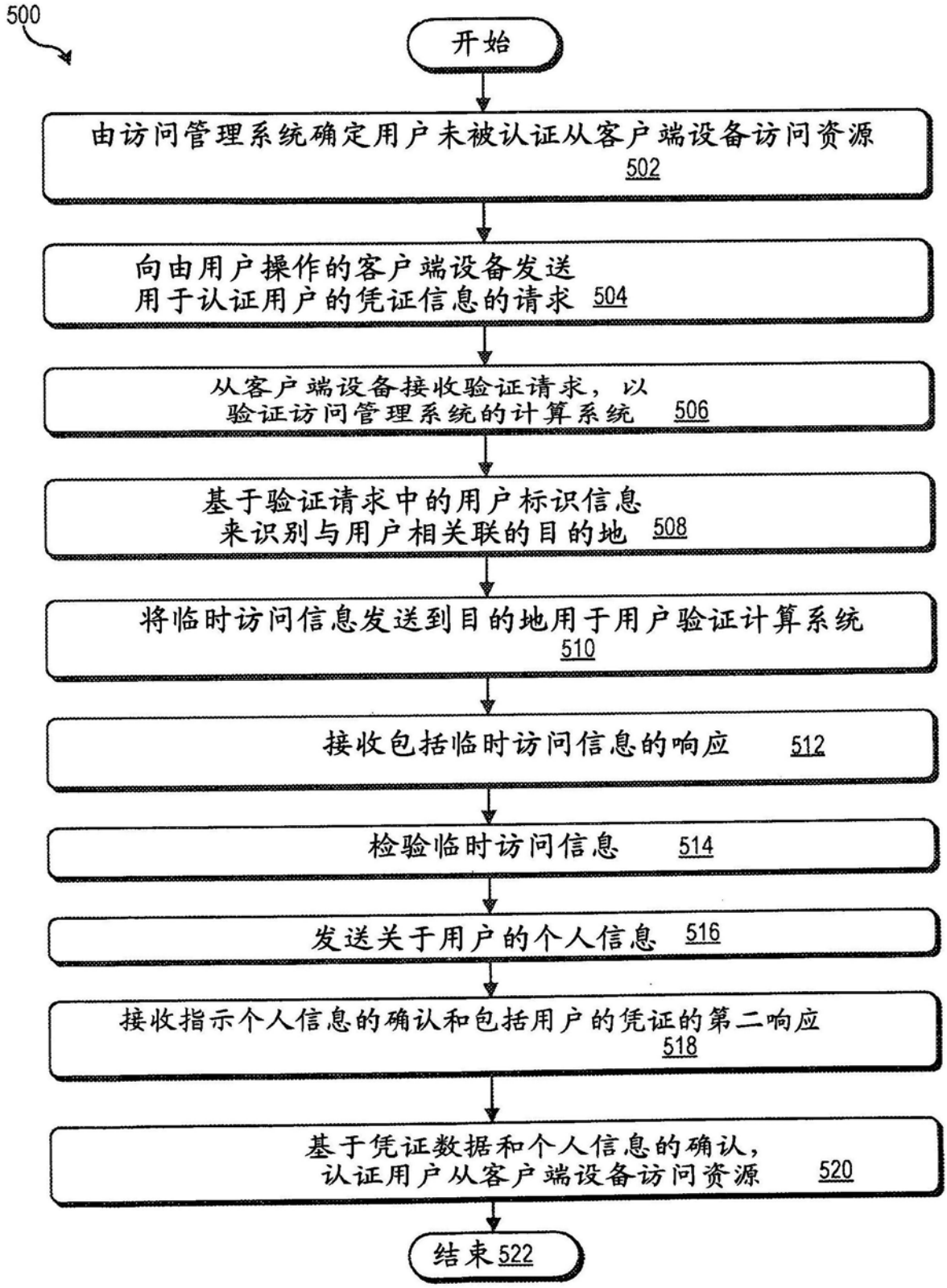

500
开始
由访问管理系统确定用户未被认证从客户端设备访问资源 502
向由用户操作的客户端设备发送 用于认证用户的凭证信息的请求 504
从客户端设备接收验证请求，以 验证访问管理系统的计算系统 506
基于验证请求中的用户标识信息 来识别与用户相关联的目的地 508
将临时访问信息发送到目的地用于用户验证计算系统 510
接收包括临时访问信息的响应 512
检验临时访问信息 514
发送关于用户的个人信息 516
接收指示个人信息的确认和包括用户的凭证的第二响应 518
基于凭证数据和个人信息的确认， 认证用户从客户端设备访问资源 520
结束 522

图5

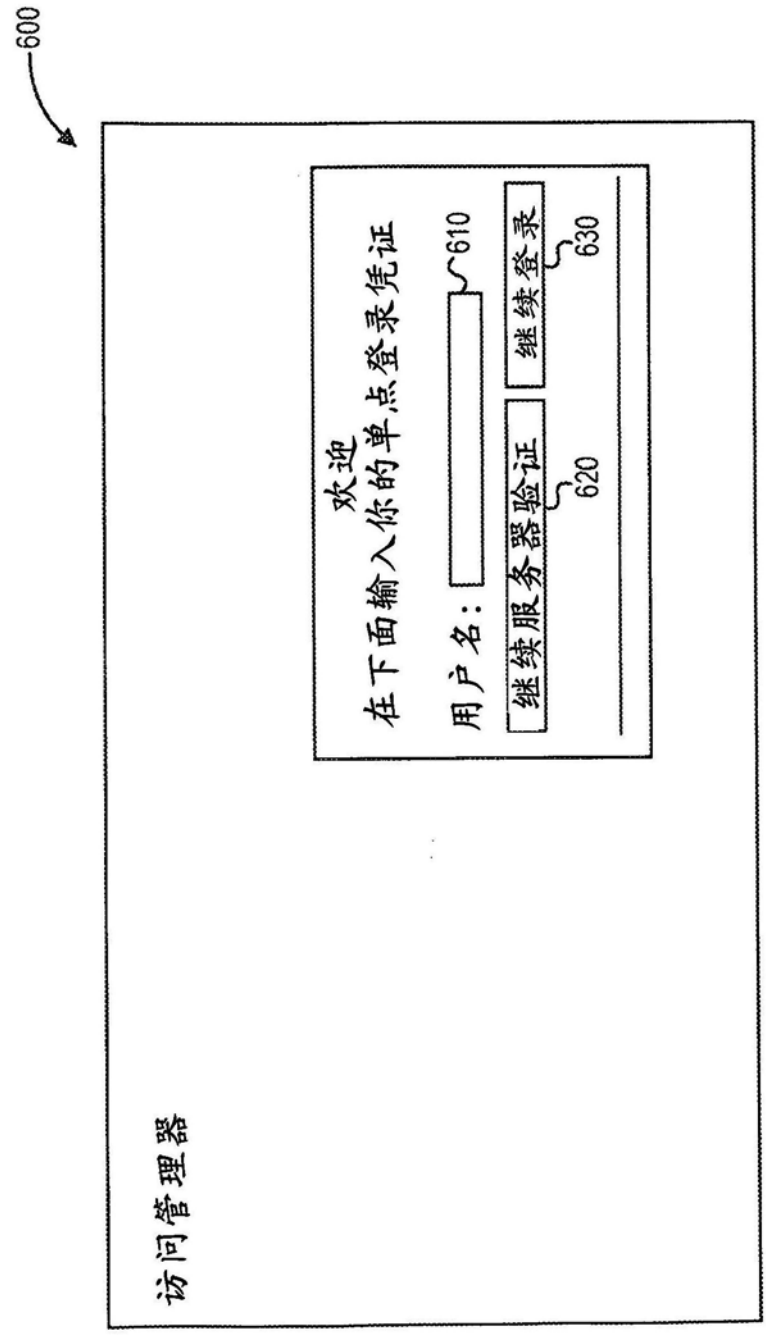


图6

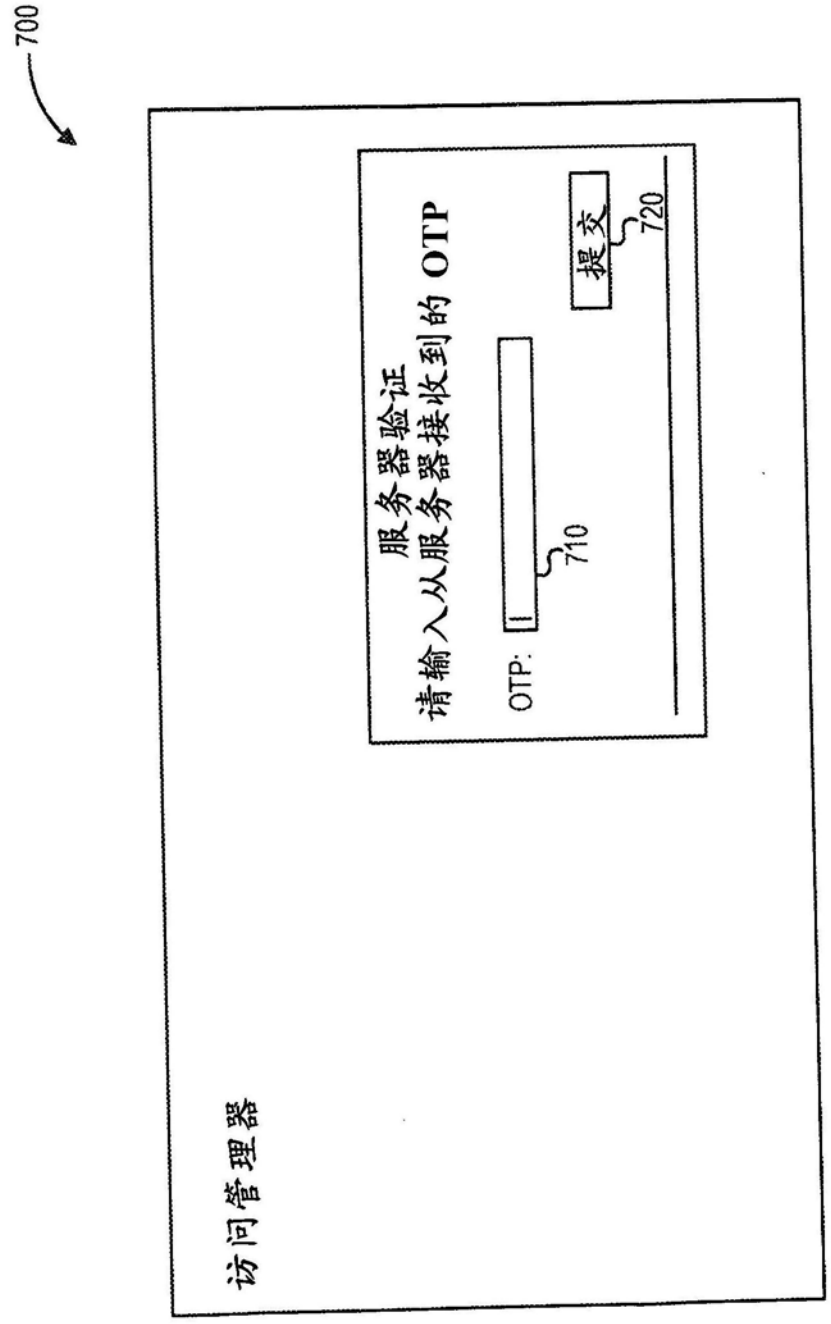


图7

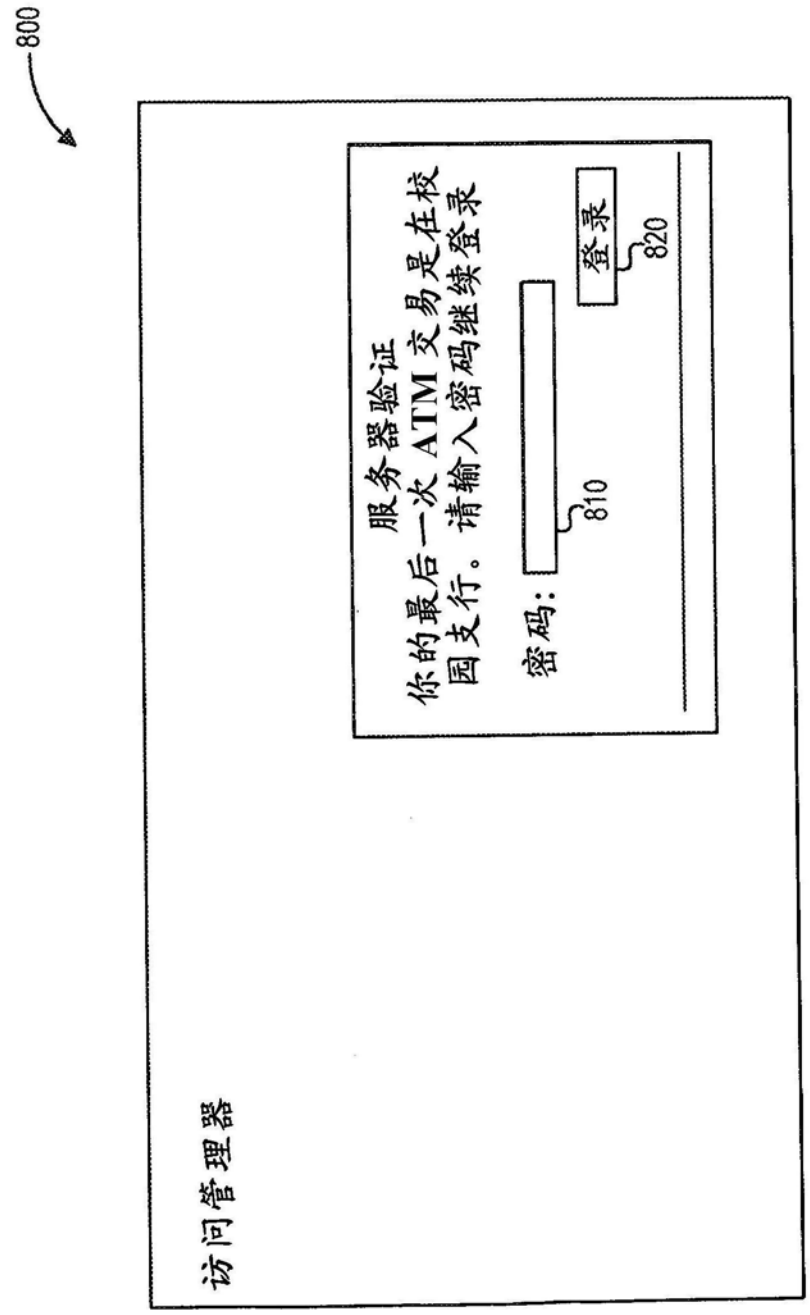


图8

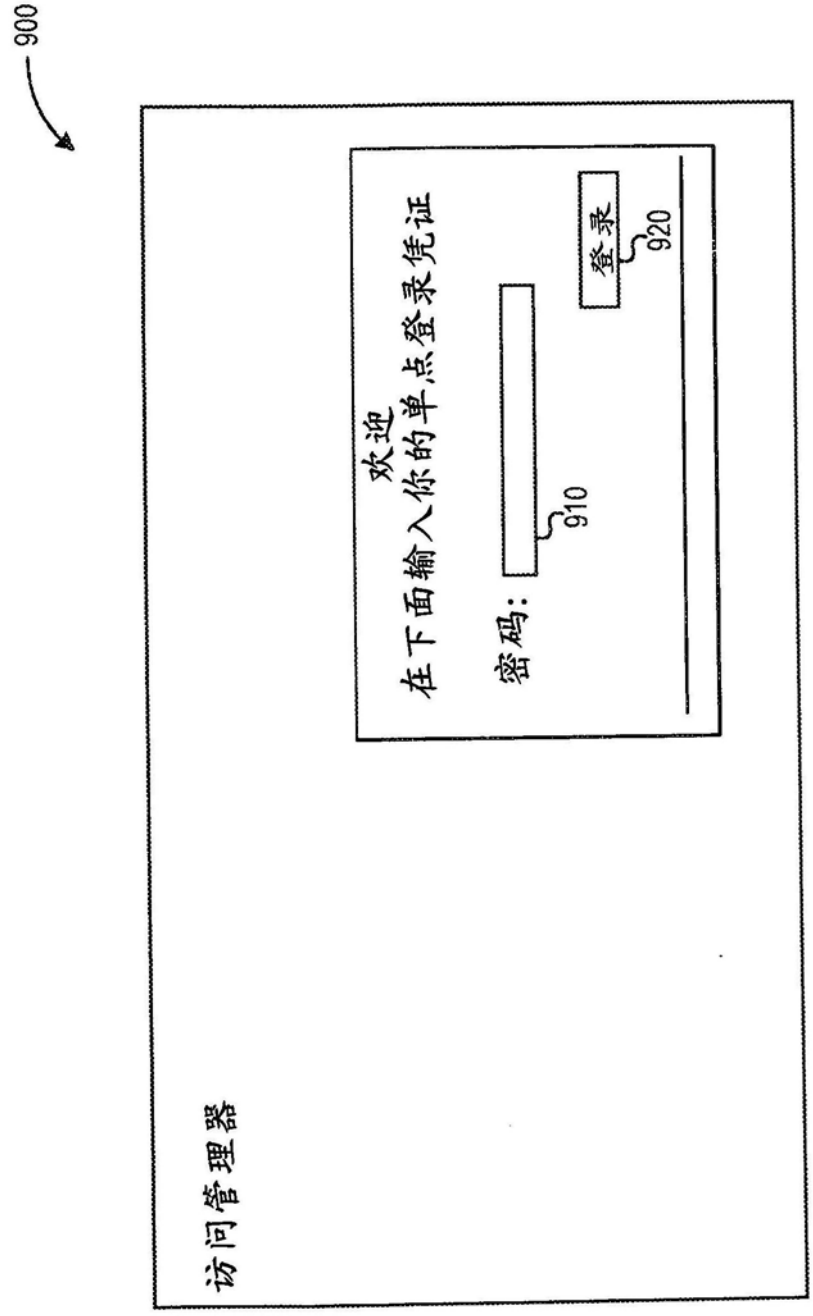


图9

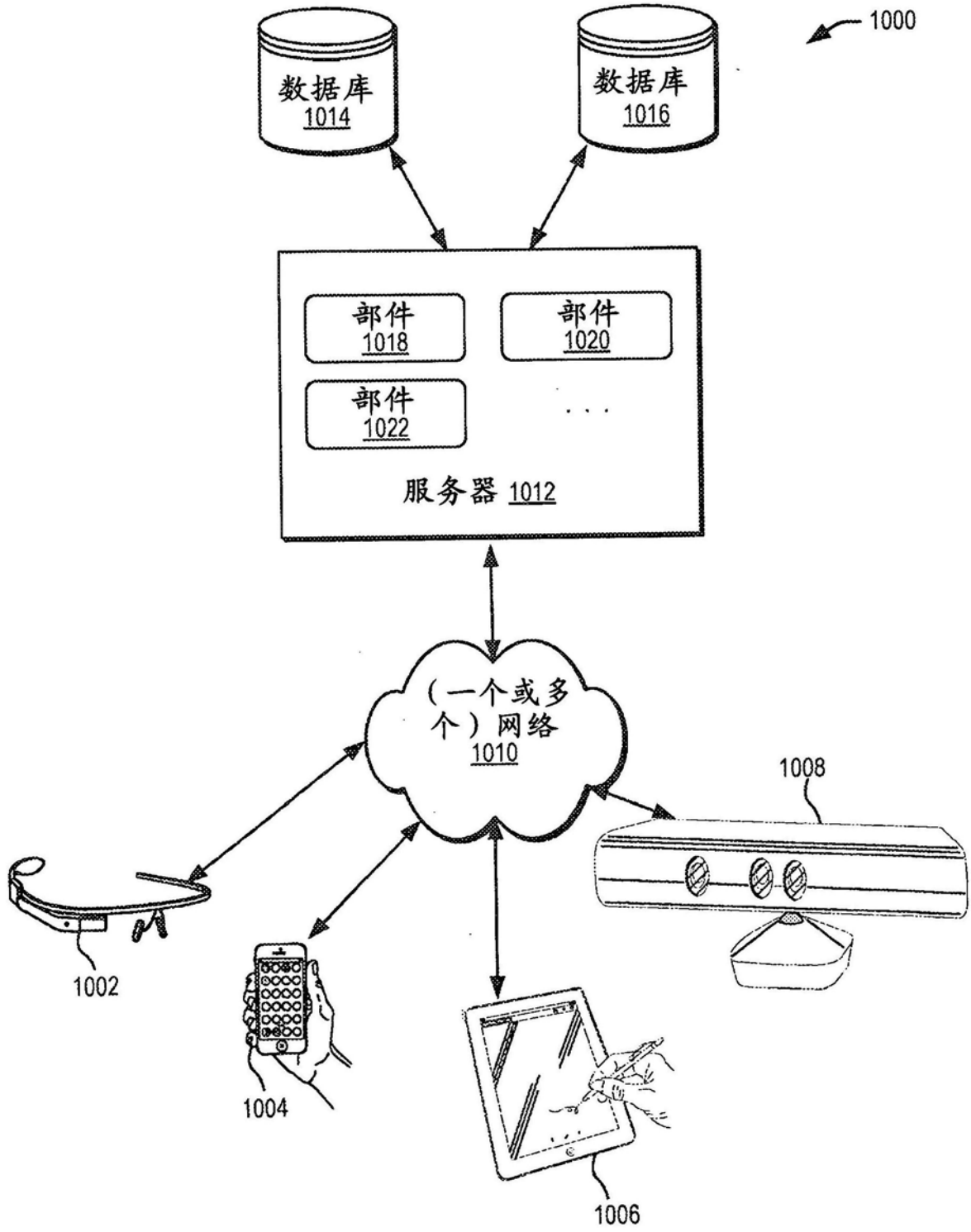

1000
数据库
1014
数据库
1016
部件
1018
部件
1020
部件
1022
. . .
服务器 1012
(一个或多个)网络
1010
1008
1002
1004
1006

图10

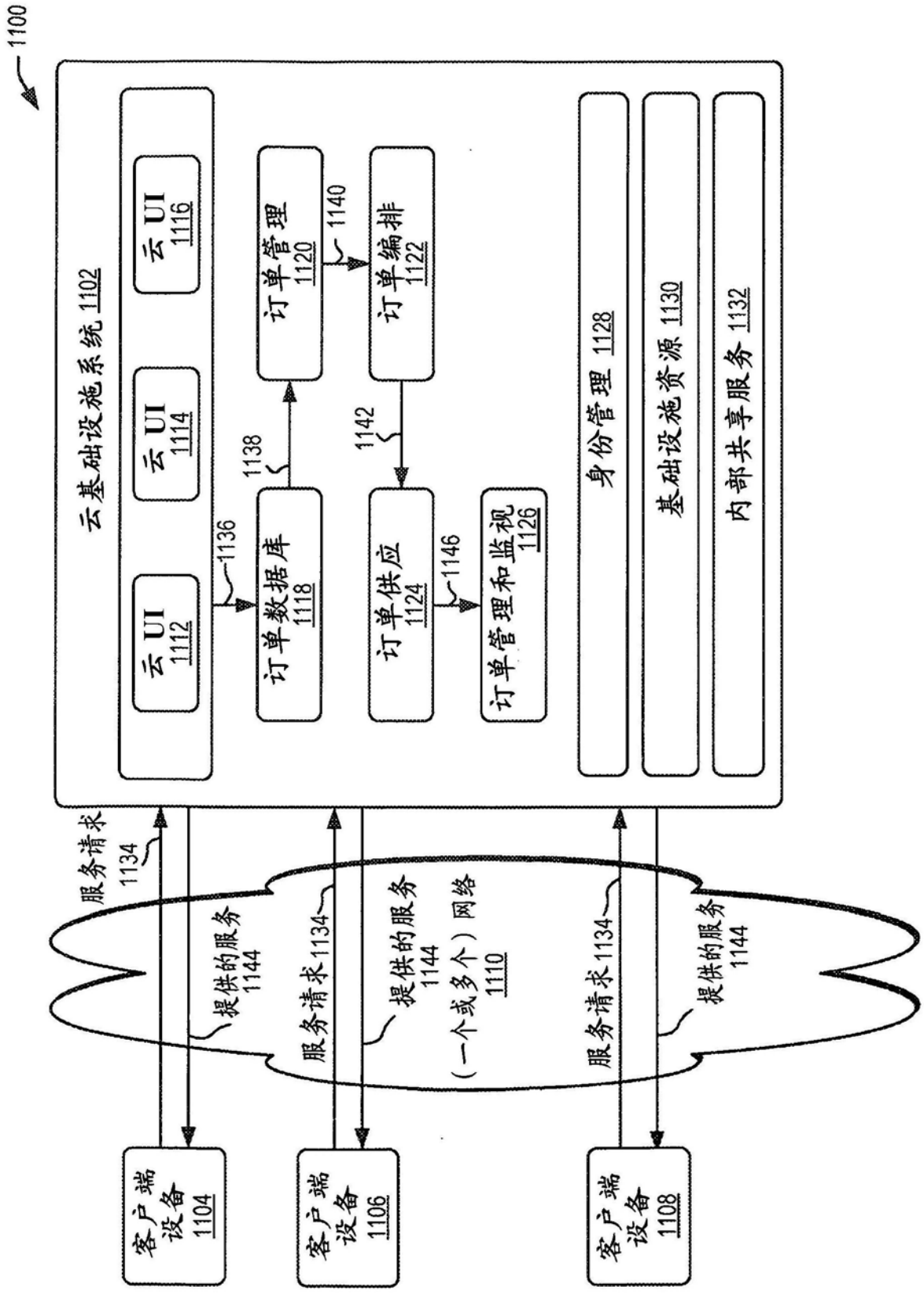

1100
云基础设施系统 1102
云 UI 1112
云 UI 1114
云 UI 1116
订单数据库 1118
订单管理 1120
订单编排 1122
订单供应 1124
订单管理和监视 1126
身份管理 1128
基础设施资源 1130
内部共享服务 1132
1136
1138
1140
1142
1146
服务请求 1134
提供的服务 1144
服务请求 1134
提供的服务 1144
（一个或多个）网络 1110
服务请求 1134
提供的服务 1144
客户端设备 1104
客户端设备 1106
客户端设备 1108

图11

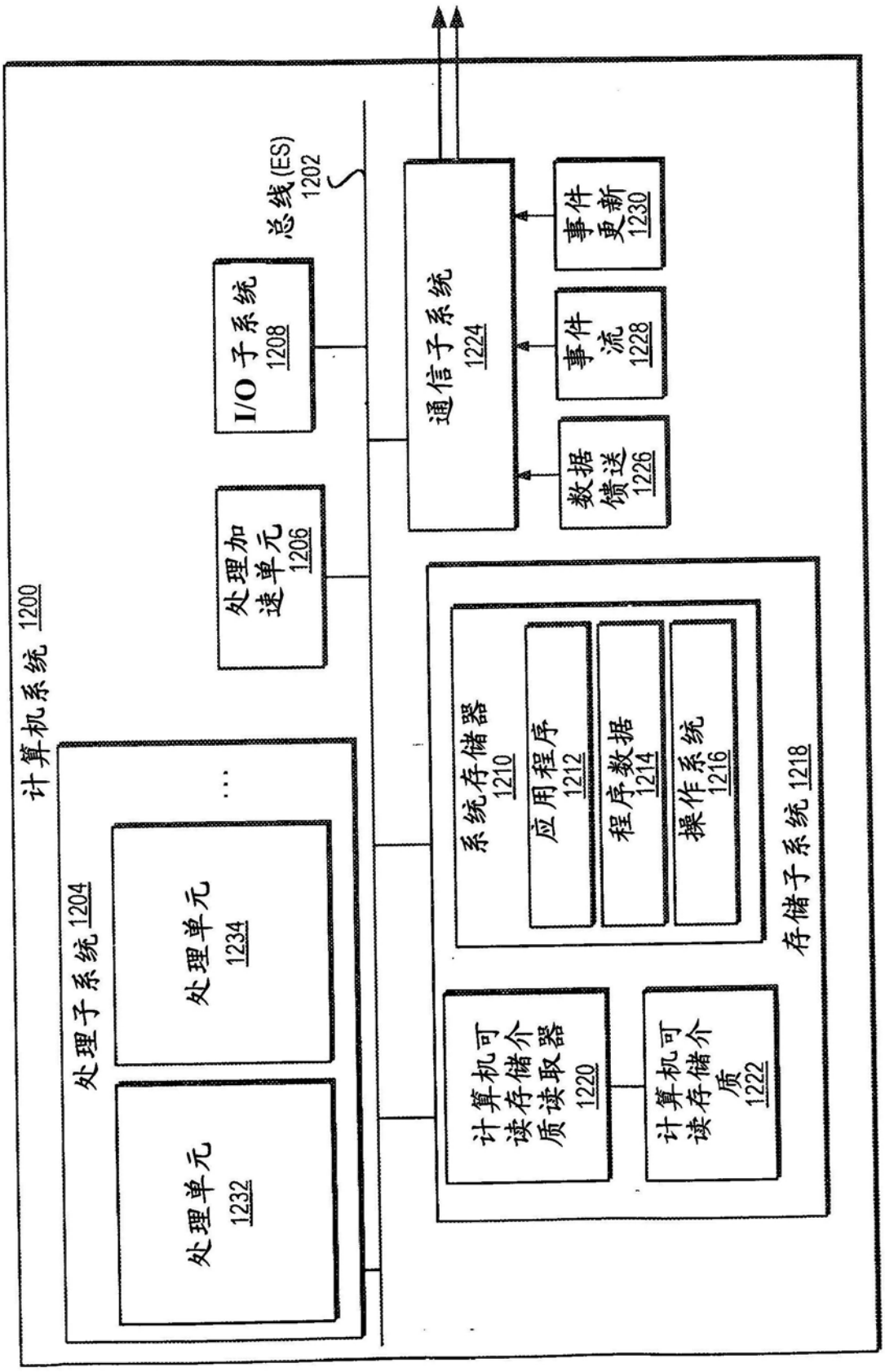

计算机系统 1200
处理子系统 1204
处理单元 1232
处理单元 1234
...
处理加速单元 1206
I/O 子系统 1208
总线(ES) 1202
通信子系统 1224
数据馈送 1226
事件流 1228
事件更新 1230
存储子系统 1218
系统存储器 1210
应用程序 1212
程序数据 1214
操作系统 1216
计算机可读存储介质读取器 1220
计算机可读存储介质 1222

图12