(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 101807992 A
(43)申请公布日 2010.08.18

(21)申请号 200910105356.0

(22)申请日 2009.02.13

(71)申请人 黄金富
地址 100032 北京市西城区金融街27号投资广场B座19层

(72)发明人 黄金富

(51)Int.Cl.
H04L 9/32(2006.01)
G06F 21/00(2006.01)

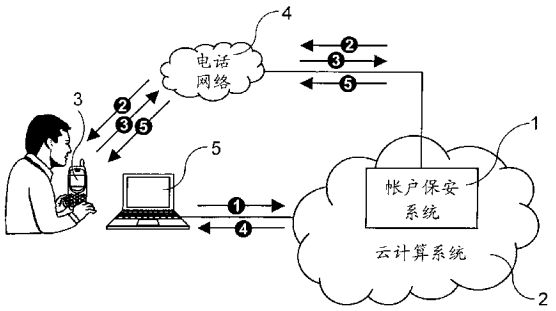
权利要求书 2 页 说明书 5 页 附图 1 页

(54)发明名称

用于云计算的帐户保安系统和方法

(57)摘要

一种用于云计算的帐户保安系统，用于保障云计算系统的帐户安全，所述系统包括位于云计算系统(2)的帐户保安系统(1)和用户手机(3)，帐户保安系统(1)监控云计算系统(2)的各帐户，当帐户保安系统(1)发现对帐户进行受监控操作时，帐户保安系统(1)通过电话网络(4)致电该帐户的用户的手机(3)，请用户输入确认信息确认，并核对用户的确认信息无误后，帐户保安系统(1)才允许云计算系统(2)进行该受监控操作请求的操作。本发明可保障云计算系统(2)的帐户安全，即使密码被黑客偷取了，没有用户手机(3)是不能对帐户进行任何受监控操作，包括登录、访问受保护数据等操作，绝对安全可靠。



CN 101807992 A

1. 一种用于云计算的帐户保安系统，用于保障云计算系统的帐户安全，其特征在于，所述的系统包括有位于云计算系统 (2) 的帐户保安系统 (1) 和各用户的手机 (3)，其中，所述的帐户保安系统 (1) 主要用于对云计算系统 (2) 中的各个帐户进行监控，当对所述的帐户进行受监控操作时，帐户保安系统 (1) 通过电话网络 (4) 致电该帐户对应的用户的手机 (3) 请求确认，并在取得该用户通过手机 (3) 发出的有效确认信息后才允许进行该受监控操作。

2. 如权利要求 1 所述的用于云计算的帐户保安系统，其特征在于，所述的受监控操作包括 :登录所述帐户和 / 或退出已登录的所述帐户和 / 或访问所述帐户内的受保护数据和 / 或下载所述帐户内的受保护数据和 / 或存储所述帐户内的受保护数据和 / 或修改所述帐户内的受保护数据。

3. 如权利要求 1 所述的用于云计算的帐户保安系统，其特征在于，所述的电话网络 (4) 包括移动电话网络和 / 或固定电话网络，所述的移动电话网络包括 GSM、CDMA、3G 之类的移动电话网络。

4. 一种用于云计算的帐户保安方法，用于保障云计算系统的帐户安全，其特征在于，所述的方法包括在云计算系统 (2) 的帐户设置限制，限制对帐户进行受监控操作，并由帐户保安系统 (1) 监控各帐户的受监控操作，当帐户保安系统 (1) 发现云计算系统 (2) 收到对云计算系统 (2) 的帐户进行受监控操作的请求时，帐户保安系统 (1) 通过电话网络 (4) 致电所述帐户对应的用户的手机 (3)，并在取得该用户通过手机 (3) 发出的有效确认信息后，帐户保安系统 (1) 才允许云计算系统 (2) 进行该受监控操作。

5. 如权利要求 4 所述的用于云计算的帐户保安方法，其特征在于，所述的受监控操作包括如下的其中一项或多项的操作 :

登录所述帐户 ;

访问所述帐户内的受保护数据 ;

下载所述帐户内的受保护数据 ;

存储所述帐户内的受保护数据 ;

修改所述帐户内的受保护数据。

6. 如权利要求 4 所述的用于云计算的帐户保安方法，其特征在于，所述的确认信息包括 :采用由用户通过手机 (3) 接听帐户保安系统 (1) 的来电作为确认信息或采用用户通过手机 (3) 接听帐户保安系统 (1) 的来电后在手机 (3) 所输入的确认密码作为确认信息。

7. 如权利要求 4 或 5 或 6 所述的用于云计算的帐户保安方法，其特征在于，所述的方法还包括对云计算系统 (2) 的帐户进行受监察操作后，帐户保安系统 (1) 通过电话网络 (4) 发短信给所述帐户的用户的手机 (3)，通知该用户有关该次受监察操作的资料。

8. 如权利要求 7 所述的用于云计算的帐户保安方法，其特征在于，所述的受监察操作包括如下的其中一项或多项的操作 :

登录所述帐户 ;

退出已登录的所述帐户 ;

访问所述帐户内的受保护数据 ;

下载所述帐户内的受保护数据 ;

存储所述帐户内的受保护数据 ;

修改所述帐户内的受保护数据。

9. 如权利要求 4 或 5 或 6 所述的用于云计算的帐户保安方法，其特征在于，所述的方法还包括如下步骤，是帐户保安系统 (1) 监控帐户进行受监控操作的步骤，具体的步骤如下：

1.) 用户使用云设备 (5) 连线到云计算系统 (2)，向云计算系统 (2) 请求对该用户的帐户进行受监控操作；

2.) 帐户保安系统 (1) 发现该操作为受监控操作，立即使用互动式语音应答装置通过电话网络 (4) 致电该帐户所对应的用户的手机 (3)；

3.) 用户从手机 (3) 的来电号码知道是帐户保安系统 (1) 的来电，接听后帐户保安系统 (1) 通过互动式语音应答装置告诉用户有关所述帐户的受监控操作的资料，如用户同意进行该受监控操作就在手机 (3) 输入确认密码，不同意就不确认输入密码；

4.) 帐户保安系统 (1) 核对用户输入的确认密码无误后，允许云计算系统 (2) 进行该受监控操作；

5.) 帐户保安系统 (1) 发短信给用户的手机 (3) 通知用户有关所述帐户该次受监控操作的资料。

10. 一种用于云计算的帐户保安方法，用于保障云计算系统的帐户安全，其特征在于，所述的方法包括云计算系统 (2) 收到对云计算系统 (2) 的帐户进行受监察操作的请求时和 / 或云计算系统 (2) 的帐户进行受监察操作后，云计算系统 (2) 通过帐户保安系统 (1) 发短信给用户的手机 (3)，通知所述帐户的用户有关该次受监察操作的资料，所述的受监察操作包括如下的其中一项或多项的操作：

登录所述帐户；

退出已登录的所述帐户；

访问所述帐户内的受保护数据；

下载所述帐户内的受保护数据；

存储所述帐户内的受保护数据；

修改所述帐户内的受保护数据。

用于云计算的帐户保安系统和方法

【技术领域】

[0001] 本发明涉及计算机及通讯技术领域，特别是涉及一种用于云计算的帐户保安系统和方法。

【背景技术】

[0002] 随着云计算(Cloud Computing)的出现，计算机网络的应用出现很大的变化，通过云计算系统，即使很复杂的计算，只要由本地计算机通过互联网发送一个需求信息到远端的云计算系统，云计算系统就会完成所需的计算，并将结果返回到本地计算机上。这样，本地计算机几乎不需要什么计算能力，所有的处理都可由远端的云计算系统来完成，把计算压力从本地计算机移到远端的云计算系统。将来，我们可能只需要一台普通的计算机，就可以通过远端的云计算系统来实现我们所需的一切，包括非常复杂的计算任务。随着云计算市场逐渐壮大，越来越多企业采用云计算系统的服务，云计算系统的安全性也越来越受到企业的关注，尤其是帐户的安全问题。由于云计算系统的无所不在特性，可大大方便了用户可在任何可连线上网的地方登录进入云计算系统的帐户，但是这种方便性却给黑客有可乘之机，如果用户的帐户密码被黑客盗用登入云计算系统，云计算系统无法分辨登录者是否就是用户本人，而用户本人也可能对帐户被盗用完全不知情，到发现时往往已经给用户造成无可挽回的损失，如何保障用户在云计算系统的帐户安全，是一个有待解决的问题。

【发明内容】

[0003] 本发明的目的，在于提供一种用于云计算的帐户保安系统和方法，以实现保障云计算系统的帐户安全的应用。

[0004] 本发明的目的是这样实现的，采用这样一种用于云计算的帐户保安系统，用于保障云计算系统的帐户安全，其特征在于，所述的系统包括有位于云计算系统 (2) 的帐户保安系统 (1) 和各用户的手机 (3)，其中，所述的帐户保安系统 (1) 主要用于对云计算系统 (2) 中的各个帐户进行监控，当对所述的帐户进行受监控操作时，帐户保安系统 (1) 通过电话网络 (4) 致电该帐户对应的用户的手机 (3) 请求确认，并在取得该用户通过手机 (3) 发出的有效确认信息后才允许进行该受监控操作。所述的受监控操作包括：登录所述帐户和 / 或退出已登录的所述帐户和 / 或访问所述帐户内的受保护数据和 / 或下载所述帐户内的受保护数据和 / 或存储所述帐户内的受保护数据和 / 或修改所述帐户内的受保护数据。

[0005] 以及，采用这样一种用于云计算的帐户保安方法，用于保障云计算系统的帐户安全，其特征在于，所述的方法包括在云计算系统 (2) 的帐户设置限制，限制对帐户进行受监控操作，并由帐户保安系统 (1) 监控各帐户的受监控操作，当帐户保安系统 (1) 发现云计算系统 (2) 收到对云计算系统 (2) 的帐户进行受监控操作的请求时，帐户保安系统 (1) 通过电话网络 (4) 致电所述帐户对应的用户的手机 (3)，并在取得该用户通过手机 (3) 发出的有效确认信息后，帐户保安系统 (1) 才允许云计算系统 (2) 进行该受监控操作。所述的受监控操作包括如下的其中一项或多项的操作：

[0006] 登录所述帐户；

[0007] 访问所述帐户内的受保护数据；

[0008] 下载所述帐户内的受保护数据；

[0009] 存储所述帐户内的受保护数据；

[0010] 修改所述帐户内的受保护数据。

[0011] 此外，还可以采用这样一种用于云计算的帐户保安方法，用于保障云计算系统的帐户安全，其特征在于，所述的方法包括云计算系统 (2) 收到对云计算系统 (2) 的帐户进行受监察操作的请求时和 / 或云计算系统 (2) 的帐户进行受监察操作后，云计算系统 (2) 通过帐户保安系统 (1) 发短信给用户的手机 (3)，通知所述帐户的用户有关该次受监察操作的资料，所述的受监察操作包括如下的其中一项或多项的操作：

[0012] 登录所述帐户；

[0013] 退出已登录的所述帐户；

[0014] 访问所述帐户内的受保护数据；

[0015] 下载所述帐户内的受保护数据；

[0016] 存储所述帐户内的受保护数据；

[0017] 修改所述帐户内的受保护数据。

[0018] 这样就实现了本发明的目的。

[0019] 本发明的帐户保安系统和方法，可以保障用户在云计算系统 (2) 的帐户安全，每次登录帐户时，都要取得用户在手机 (3) 输入的确认信息后，云计算系统 (2) 才允许进行该次登录的操作，如果用户的密码被黑客偷取了，没有用户的手机 (3) 就无法进行登录操作，也就无法盗取帐户内数据。

【附图说明】

[0020] 图 1 是本发明的帐户保安系统的示意说明图；

[0021] 图 2 是本发明的帐户保安方法的步骤示意说明图。

[0022] 图中，相同的数字代表相同的系统、装置、部件器件，方法步骤用圆圈的数字和带箭头的直线所标出。附图是示意性的，用以说明本发明的系统和方法的主要特征。

【具体实施方式】

[0023] 下面结合附图，对本发明的方法作进一步详细说明。

[0024] 参阅图 1，图 1 是本发明的帐户保安系统的示意说明图，图中示出的系统包括有位于云计算系统 (2) 的帐户保安系统 (1) 和各用户的手机 (3)，其中，所述的帐户保安系统 (1) 主要用于对云计算系统 (2) 中的各个帐户进行监控，当对所述的帐户进行受监控操作时，帐户保安系统 (1) 通过电话网络 (4) 致电该帐户对应的用户的手机 (3) 请求确认，并在取得该用户通过手机 (3) 发出的有效确认信息后才允许进行该受监控操作。所述的受监控操作包括：登录所述帐户和 / 或退出已登录的所述帐户和 / 或访问所述帐户内的受保护数据和 / 或下载所述帐户内的受保护数据和 / 或存储所述帐户内的受保护数据和 / 或修改所述帐户内的受保护数据。

[0025] 在设置方面，帐户保安系统 (1) 设有连接电话网络 (4) 的互动式语音应答 (IVR,

Interactive Voice Response)装置，用户要在帐户保安系统(1)登记自己的手机(3)电话号码，将该手机(3)电话号码与用户的帐户相捆绑，并选择一个用于确认的确认信息，可以采用由用户通过手机(3)接听帐户保安系统(1)的来电作为确认信息，或者由用户设定一个确认密码，当帐户保安系统(1)致电用户的手机(3)请求确认时，用户通过手机(3)接听该来电后在手机(3)输入该确认密码，所输入的该确认密码就作为确认信息，以后对该帐户进行受监控操作时，帐户保安系统(1)会自动致电给用户，并在取得用户在手机(3)输入有效的确认信息后才允许进行该次受监控操作。此外，用户还可以将帐户内的部分数据设定为受保护数据，当对这些受保护数据进行访问、下载、存储、修改等操作时，帐户保安系统(1)也会自动致电给用户，要求用户通过手机(3)输入确认信息再次确认，确认成功后才允许对这些受保护数据进行访问、下载、存储、修改等操作。

[0026] 参阅图2，图2是本发明的帐户保安方法的步骤示意说明图，图中示出的方法包括在云计算系统(2)的帐户设置限制，限制对帐户进行受监控操作，并由帐户保安系统(1)监控各帐户的受监控操作，当帐户保安系统(1)发现云计算系统(2)收到对云计算系统(2)的帐户进行受监控操作的请求时，帐户保安系统(1)通过电话网络(4)致电所述帐户对应的用户的手机(3)，并在取得该用户通过手机(3)发出的有效确认信息后，帐户保安系统(1)才允许云计算系统(2)进行该受监控操作。所述的确认信息包括：采用由用户通过手机(3)接听帐户保安系统(1)的来电作为确认信息或采用用户通过手机(3)接听帐户保安系统(1)的来电后在手机(3)所输入的确认密码作为确认信息。以及，所述的受监控操作包括如下的其中一项或多项的操作：

[0027] 1. 登录所述帐户；

[0028] 2. 访问所述帐户内的受保护数据；

[0029] 3. 下载所述帐户内的受保护数据；

[0030] 4. 存储所述帐户内的受保护数据；

[0031] 5. 修改所述帐户内的受保护数据。

[0032] 例如，受监控操作只包括上述的第1项，每次登录进入用户的帐户时，帐户保安系统(1)都会通过电话网络(4)致电用户的手机(3)，并在取得该用户通过手机(3)发出的有效确认信息后，帐户保安系统(1)才允许云计算系统(2)让用户登录进入帐户。又例如，受监控操作包括上述的第1、3项，每次登录进入用户的帐户或从帐户中下载受保护数据，帐户保安系统(1)都会通过电话网络(4)致电用户的手机(3)，并在取得该用户通过手机(3)发出的有效确认信息后，帐户保安系统(1)才允许云计算系统(2)让用户登录进入帐户或下载受保护数据。无论受监控操作只包括上述的其中任一项、或任两项、或任三项、或任四项、或全部各项，都可很好地实现本发明的目的，都是属于本发明的保护范围。

[0033] 在本发明的帐户保安方法中，所述的受保护数据包括用户登录进入云计算系统(2)的帐户后才能看到的数据即受保护私人数据，或用户开放给其他用户存取的数据即受保护共享数据，查看受保护共享数据时是无须登录进入用户的帐户，只要查看者登录进入查看者自己的帐户，然后向云计算系统(2)要求查看其他人的受保护共享数据，帐户保安系统(1)就会自动通过电话网络(4)致电用户的手机(3)，通知用户有关查看者的身份和受保护共享数据的资料，并在取得该用户通过手机(3)发出的有效确认信息后，帐户保安系统(1)才允许云计算系统(2)让查看者查看该受保护共享数据。这样用户就可将一些私

人资料在有需要时，公开给指定的人查看。例如将本发明的帐户保安方法应用于电子病历数据库，病人可以将自己的部分或全部病历数据设定为受保护共享数据，然后在看医生时，由病人自己通过手机 (3) 确认让医生查看该受保护共享数据，既可保障病人的私隐不会被其他人看到，又可方便医生诊症。又例如将本发明的帐户保安方法应用于个人信用数据库，将用户的部分或全部信用数据设定为受保护共享数据，当有人要查看用户的个人信用数据时，由用户通过自己的手机 (3) 确认让该查看者查看该受保护共享数据，既可保障用户的个人私隐不会被其他人看到，又可于需要时为用户提供经过个人信用数据库认证的信用数据给用户指定的查看者查看。

[0034] 继续参阅图 2，图 2 示出的方法还包括对云计算系统 (2) 的帐户进行受监察操作后，帐户保安系统 (1) 通过电话网络 (4) 发短信给所述帐户的用户的手机 (3)，通知该用户有关该次受监察操作的资料，所述的受监察操作包括如下的其中一项或多项的操作：

[0035] A. 登录所述帐户；

[0036] B 退出已登录的所述帐户；

[0037] C. 访问所述帐户内的受保护数据；

[0038] D. 下载所述帐户内的受保护数据；

[0039] E. 存储所述帐户内的受保护数据；

[0040] F. 修改所述帐户内的受保护数据。

[0041] 例如，受监察操作只包括上述的第 A 项，每次登录进入用户的帐户时，帐户保安系统 (1) 都会通过电话网络 (4) 发短信给用户的手机 (3)，通知用户有人登录进入他的帐户。又例如，受监察操作包括上述的第 A、B 项，每次登录进入用户的帐户或退出已登录的帐户时，帐户保安系统 (1) 都会通过电话网络 (4) 发短信给用户的手机 (3)，通知用户有人登录进入他的帐户或已退出他的帐户。无论受监察操作只包括上述的其中任一项、或任两项、或任三项、或任四项、或任五项、或全部各项，都可很好地实现本发明的目的，都是属于本发明的保护范围。

[0042] 继续参阅图 2，图 2 示出的方法还包括如下步骤，是帐户保安系统 (1) 监控帐户进行受监控操作的步骤，具体的步骤如下：

[0043] 1. 用户使用云设备 (5) 连线到云计算系统 (2)，向云计算系统 (2) 请求对该用户的帐户进行受监控操作；

[0044] 2. 帐户保安系统 (1) 发现该操作为受监控操作，立即使用互动式语音应答装置通过电话网络 (4) 致电该帐户所对应的用户的手机 (3)；

[0045] 3. 用户从手机 (3) 的来电号码知道是帐户保安系统 (1) 的来电，接听后帐户保安系统 (1) 通过互动式语音应答装置告诉用户有关所述帐户的受监控操作的资料，如用户同意进行该受监控操作就在手机 (3) 输入确认密码，不同意就不确认输入密码；

[0046] 4. 帐户保安系统 (1) 核对用户输入的确认密码无误后，允许云计算系统 (2) 进行该受监控操作；

[0047] 5. 帐户保安系统 (1) 发短信给用户的手机 (3) 通知用户有关所述帐户该次受监控操作的资料。

[0048] 以上的帐户保安方法是采用另路确认方法，通过电话网络 (4) 与用户的手机 (3) 交换信息，并在收到用户通过手机 (3) 发出有效的确认信息后，才允许进行受监控操作。在

本说明书中，所述的电话网络 (4) 包括移动电话网络和 / 或固定电话网络，所述的移动电话网络包括 GSM、CDMA、3G 之类的移动电话网络。由于电话网络 (4) 是独立于云计算系统 (2) 所连接的计算机网络，所以即使用户的登录密码被黑客偷取了，黑客没有用户的手机 (3) 就无法进行任何一项受监控操作，也就无法盗取帐户内的重要数据。这种采用另路确认的帐户保安方法，能有效保障云计算系统 (2) 的帐户的安全。

[0049] 此外，除了采用以上的方法保障帐户的安全外，也可以采用简单的警觉提示方法来保障帐户安全，是在每次对帐户进行受监察的操作时，发短信通知用户，如果用户收到短信但并没有进行受监察的操作，表示他的帐户可能被人盗用，用户就可立即采取行动，减少帐户被盗用造成的损失。这种采用警觉提示的帐户保安方法，包括云计算系统 (2) 收到对云计算系统 (2) 的帐户进行受监察操作的请求时和 / 或云计算系统 (2) 的帐户进行受监察操作后，云计算系统 (2) 通过帐户保安系统 (1) 发短信给用户的手机 (3)，通知所述帐户的用户有关该次受监察操作的资料，所述的受监察操作包括如下的其中一项或多项的操作 ：

[0050] A. 登录所述帐户 ；

[0051] B. 退出已登录的所述帐户 ；

[0052] C. 访问所述帐户内的受保护数据 ；

[0053] D. 下载所述帐户内的受保护数据 ；

[0054] E. 存储所述帐户内的受保护数据 ；

[0055] F. 修改所述帐户内的受保护数据。

[0056] 这种采用警觉提示的帐户保安方法，用户可以如常地对帐户进行受监察的操作，无须进行任何额外的步骤，用户只会在进行受监察的操作后收到警觉提示的短信，由用户自己判断帐户是否被盗用，只要帐户被别人盗用，用户就可立即知晓，就可立即采取行动避免损失，同样也可达到保障帐户安全的效用。虽然本方法比图 2 所采用通过手机 (3) 确认的帐户保安方法安全性稍逊，但是在操作上却简单得多，本方法已可满足大部分用户对安全性的要求，而图 2 所采用通过手机 (3) 确认的帐户保安方法则适合于一些对安全性要求极高的应用。

[0057] 本发明的帐户保安系统和帐户保安方法除了可应用于云计算系统 (2) 外，也可以应用于其他设有帐户的设备系统中，包括设有数据库的计算机，设有帐户的服务器等。在本说明书中，云计算系统 (2) 包括采用云计算 (Cloud Computing) 的计算机系统、采用云计算 (Cloud Computing) 的计算机网络、设有帐户的服务器、设有数据库的计算机、设有数据库的服务器等。无论将本发明的帐户保安系统或帐户保安方法应用于以上的任一系统或计算机或服务器，都可很好地实现本发明的目的，都是属于本发明的保护范围。

[0058] 以上已经详细说明本发明的帐户保安系统和方法，虽然本发明以上述的实施例加以说明，但是本发明并不仅限于此，在不离开本发明的精神和所附权利要求书的范围的情况下，可以作多种改变和变化，例如将帐户保安系统 (1) 的功能整合到云计算系统 (2) 中，都可很好地实现本发明的目的，都是属于本发明的保护范围。

[0059] 本发明能有效改善云计算系统的安全性，它的实施，会带来良好的社会效益和经济效益。

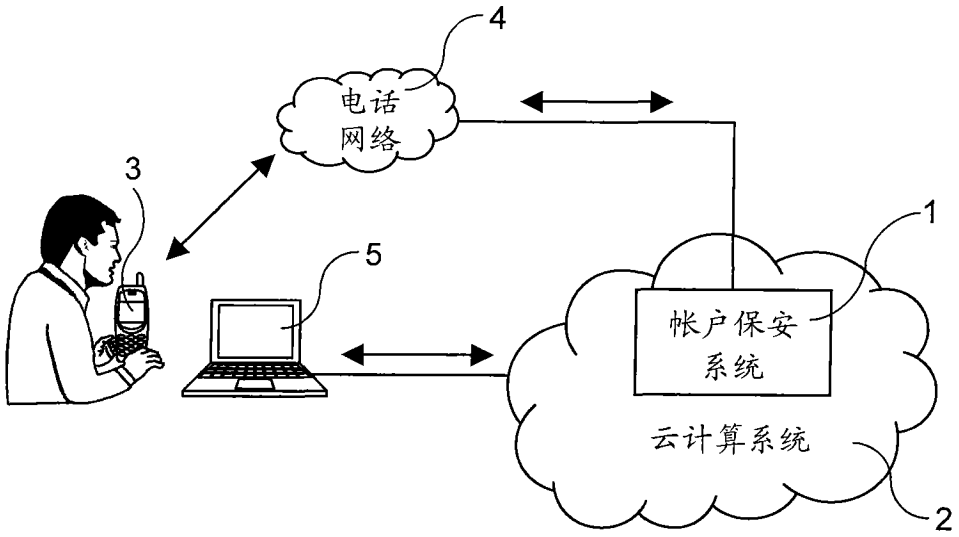


图 1

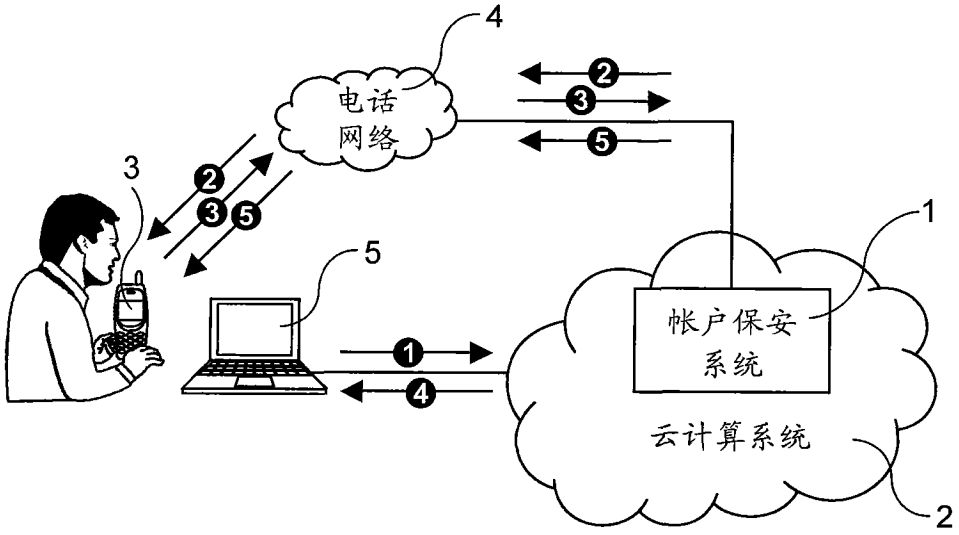


图 2