(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 101807993 A
(43)申请公布日 2010.08.18

(21)申请号 200910105357.5

(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)

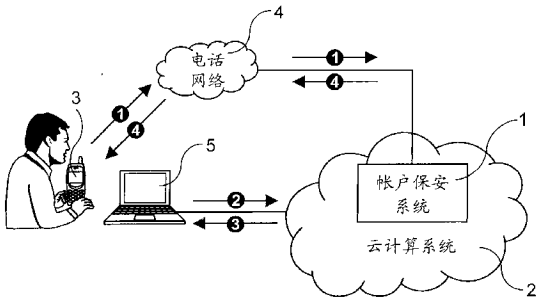
权利要求书 2 页 说明书 5 页 附图 1 页

(54)发明名称

用于云计算采用上锁开锁机制的帐户保安系统和方法

(57)摘要

一种用于云计算采用上锁开锁机制的帐户保安系统，用于保障云计算系统的帐户安全，所述的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)内设有多个用于指示帐户状态的状态标志，当对云计算系统(2)的帐户进行受监控操作时，云计算系统(2)向帐户保安系统(1)查询该帐户对应的状态标志的状态，只有在帐户保安系统(1)回答该状态标志的状态为“开锁”时，云计算系统(2)才允许进行该项受监控操作。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，黑客没有用户手机(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 101807993 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) 内设有多个用于指示帐户状态的状态标志，每一状态标志分别对应云计算系统 (2) 的其中一个帐户及对应其中一手机 (3) 电话号码，当对云计算系统 (2) 的帐户进行受监控操作时，云计算系统 (2) 向帐户保安系统 (1) 查询该帐户对应的状态标志的状态，只有在帐户保安系统 (1) 回答该状态标志的状态为“开锁”时，云计算系统 (2) 才允许进行该项受监控操作，以及，所述的手机 (3) 通过电话网络 (4) 与帐户保安系统 (1) 交换信息，包括从手机 (3) 发送给帐户保安系统 (1) 的开锁信息和 / 或从帐户保安系统 (1) 发送给手机 (3) 的警觉信息，所述的开锁信息用于指示帐户保安系统 (1) 将该手机 (3) 所对应的状态标志的设置为“开锁”状态。

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，当云计算系统 (2) 收到对帐户进行受监控操作的指令时，云计算系统 (2) 向帐户保安系统 (1) 查询该帐户对应的状态标志的状态，只有在帐户保安系统 (1) 回答该状态标志是处于“开锁”状态时，云计算系统 (2) 才允许进行该项受监控操作，以及，帐户保安系统 (1) 内各个状态标志平常是处于“上锁”状态，只有收到由手机 (3) 发出的有效开锁信息时，帐户保安系统 (1) 才将该手机 (3) 所对应的状态标志设置为“开锁”状态一段指定时间，该段指定时间过后帐户保安系统 (1) 自动将该状态标志设置为“上锁”状态。

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，所述的云计算系统 (2) 向帐户保安系统 (1) 查询某一帐户对应的状态标志的状态时，帐户保安系统 (1) 向云计算系统 (2) 回答将该状态标志的状态，然后帐户保安系统 (1) 将该状态标志设置为“上锁”状态。

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。

7. 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，所述的开锁信息包括 :采用帐户保安系统 (1) 接收到用户手机 (3) 的来电呼叫作为开锁信息或采用帐户保安系统 (1) 接听用户手机 (3) 的来电后用户在手机 (3) 所输入的开锁密码作为开锁信息或采

用由用户手机 (3) 所发送到帐户保安系统 (1) 包含有开锁密码的短信为开锁信息或采用由用户手机 (3) 所发送到帐户保安系统 (1) 包含有开锁密码的彩信为开锁信息。

8. 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，所述的方法还包括云计算系统 (2) 向帐户保安系统 (1) 查询某一帐户对应的状态标志的状态后，帐户保安系统 (1) 通过电话网络 (4) 发短信给该帐户对应的用户手机 (3)，通知用户有关该次的查询。

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) 监控对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)，对该用户的帐户进行受监控操作前，用户使用手机 (3) 致电帐户保安系统 (1)，拨通后就可立即挂线；

帐户保安系统 (1) 从来电的电话号码找出对应该电话号码的状态标志，然后将该状态标志设置为“开锁”状态一段指定时间，并在该段指定时间过后自动将该状态标志设置为“上锁”状态；

2.) 用户在该段指定时间期间，使用云设备 (5) 向云计算系统 (2) 发出要求对该用户的帐户进行受监控操作，云计算系统 (2) 收到该要求后向帐户保安系统 (1) 查询该帐户对应的状态标志的状态；

3.) 帐户保安系统 (1) 找出该帐户对应的状态标志的状态，由于用户是在该段指定时间期间发出该请求，所以状态标志处于“开锁”状态，帐户保安系统 (1) 将该“开锁”状态信息传送给云计算系统 (2)，然后帐户保安系统 (1) 将该状态标志设置为“上锁”状态，以及，云计算系统 (2) 收到该“开锁”状态信息后允许进行该次受监控操作；

4.) 帐户保安系统 (1) 发短信给用户的手机 (3) 通知用户该帐户进行了一次受监控操作。

用于云计算采用上锁开锁机制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采用上锁开锁机制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采用上锁开锁机制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) 内设有多个用于指示帐户状态的状态标志，每一状态标志分别对应云计算系统 (2) 的其中一个帐户及对应其中一手机 (3) 电话号码，当对云计算系统 (2) 的帐户进行受监控操作时，云计算系统 (2) 向帐户保安系统 (1) 查询该帐户对应的状态标志的状态，只有在帐户保安系统 (1) 回答该状态标志的状态为“开锁”时，云计算系统 (2) 才允许进行该项受监控操作，以及，所述的手机 (3) 通过电话网络 (4) 与帐户保安系统 (1) 交换信息，包括从手机 (3) 发送给帐户保安系统 (1) 的开锁信息和 / 或从帐户保安系统 (1) 发送给手机 (3) 的警觉信息，所述的开锁信息用于指示帐户保安系统 (1) 将该手机 (3) 所对应的状态标志的设置为“开锁”状态。

[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，当云计算系统 (2) 收到对帐户进行受监控操作的指令时，云计算系统 (2) 向帐户保安系统 (1) 查询该帐户对应的状态标志的状态，只有在帐户保安系统 (1) 回答该状态标志是处于“开锁”状态时，云计算系统 (2) 才允许进行该项受监控操作，以及，帐户保安系统

(1) 内各个状态标志平常是处于“上锁”状态，只有收到由手机 (3) 发出的有效开锁信息时，帐户保安系统 (1) 才将该手机 (3) 所对应的状态标志设置为“开锁”状态一段指定时间，该段指定时间过后帐户保安系统 (1) 自动将该状态标志设置为“上锁”状态。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] 这样就实现了本发明的目的。

[0012] 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，每次登录云计算系统 (2) 的帐户前，都要预先使用用户的手机 (3) 向帐户保安系统 (1) 发出有效的开锁信息将该帐户对应的状态标志设置为“开锁”状态，才能成功登录进入帐户，即使用户的密码被黑客偷取了，黑客没有用户的手机 (3) 就无法“开锁”，也就无法登录进入用户的帐户。

【附图说明】

[0013] 图 1 是本发明的帐户保安系统的示意说明图；

[0014] 图 2 是本发明的帐户保安方法的步骤示意说明图。

[0015] 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】

[0016] 下面结合附图，对本发明的方法作进一步详细说明。

[0017] 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) 内设有多个用于指示帐户状态的状态标志，每一状态标志分别对应云计算系统 (2) 的其中一个帐户及对应其中一手机 (3) 电话号码，当对云计算系统 (2) 的帐户进行受监控操作时，云计算系统 (2) 向帐户保安系统 (1) 查询该帐户对应的状态标志的状态，只有在帐户保安系统 (1) 回答该状态标志的状态为“开锁”时，云计算系统 (2) 才允许进行该项受监控操作，以及，所述的手机 (3) 通过电话网络 (4) 与帐户保安系统 (1) 交换信息，包括从手机 (3) 发送给帐户保安系统 (1) 的开锁信息和 / 或从帐户保安系统 (1) 发送给手机 (3) 的警觉信息，所述的开锁信息用于指示帐户保安系统 (1) 将该手机 (3) 所对应的状态标志的设置为“开锁”状态。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。

[0018] 在设置方面，帐户保安系统 (1) 设有连接电话网络 (4) 的线路和装置，并设有多个用于指示帐户状态的状态标志，每一状态标志分别对应云计算系统 (2) 的其中一个帐户，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

在云计算系统 (2) 的帐户及状态标志相捆绑，并选择设定一个用于开锁的开锁信息，可以采用帐户保安系统 (1) 接收到用户手机 (3) 的来电呼叫作为开锁信息或采用帐户保安系统 (1) 接听用户手机 (3) 的来电后用户在手机 (3) 所输入的开锁密码作为开锁信息或采用由用户手机 (3) 所发送到帐户保安系统 (1) 包含有开锁密码的短信为开锁信息或采用由用户手机 (3) 所发送到帐户保安系统 (1) 包含有开锁密码的彩信为开锁信息等等，以后对该帐户进行指定的受监控操作前，用户要预先使用手机 (3) 向帐户保安系统 (1) 发出有效的开锁信息将该帐户对应的状态标志设置为“开锁”状态，云计算系统 (2) 才允许继续进行该受监控操作。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、修改等操作前，用户要预先将该帐户对应的状态标志设置为“开锁”状态，才能对这些受保护数据进行访问、下载、存储、修改等操作。

[0019] 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，当云计算系统 (2) 收到对帐户进行受监控操作的指令时，云计算系统 (2) 向帐户保安系统 (1) 查询该帐户对应的状态标志的状态，只有在帐户保安系统 (1) 回答该状态标志是处于“开锁”状态时，云计算系统 (2) 才允许进行该项受监控操作，以及，帐户保安系统 (1) 内各个状态标志平常是处于“上锁”状态，只有收到由手机 (3) 发出的有效开锁信息时，帐户保安系统 (1) 才将该手机 (3) 所对应的状态标志设置为“开锁”状态一段指定时间 (例如指定时间为 3 分钟)，该段指定时间过后帐户保安系统 (1) 自动将该状态标志设置为“上锁”状态。所述的开锁信息包括 :采用帐户保安系统 (1) 接收到用户手机 (3) 的来电呼叫作为开锁信息或采用帐户保安系统 (1) 接听用户手机 (3) 的来电后用户在手机 (3) 所输入的开锁密码作为开锁信息或采用由用户手机 (3) 所发送到帐户保安系统 (1) 包含有开锁密码的短信为开锁信息或采用由用户手机 (3) 所发送到帐户保安系统 (1) 包含有开锁密码的彩信为开锁信息。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 :

[0020] 1. 登录所述帐户 ;

[0021] 2. 访问所述帐户内的受保护数据 ;

[0022] 3. 下载所述帐户内的受保护数据 ;

[0023] 4. 存储所述帐户内的受保护数据 ;

[0024] 5. 修改所述帐户内的受保护数据。

[0025] 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，云计算系统 (2) 都会向帐户保安系统 (1) 查询该帐户对应的状态标志的状态，只有帐户保安系统 (1) 回答该状态标志为“开锁”状态时，才允许用户登录进入帐户。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时，云计算系统 (2) 都会向帐户保安系统 (1) 查询该帐户对应的状态标志的状态，只有帐户保安系统 (1) 回答该状态标志为“开锁”状态时，才允许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。

[0026] 本发明的帐户保安方法的更进一步改进，是在云计算系统 (2) 向帐户保安系统 (1) 查询某一帐户对应的状态标志的状态时，帐户保安系统 (1) 向云计算系统 (2) 回答将该状态标志的状态，然后帐户保安系统 (1) 将该状态标志设置为“上锁”状态。这样每一次开

锁操作只供一次受监控操作使用，可进一步改进本发明的安全性。

[0027] 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，同时用户要预先使用手机(3)向帐户保安系统(1)发出有效的开锁信息将该帐户对应的状态标志设置为“开锁”状态，查看者就可以在该“开锁”状态期间查看到该受保护共享数据。这样用户就可将一些私人资料在有需要时，公开给其他人查看，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，由病人预先通过自己的手机(3)将自己的电子病历数据库帐户对应的状态标志设置为“开锁”状态，认让医生在该“开锁”状态期间查看该受保护共享数据，而在医生查看该受保护共享数据后，帐户保安系统(1)更可将查看者的身份和所查看过的受保护共享数据的简要，通过发短信给病人的手机(3)通知病人，这样既可保障病人的私隐，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，由用户预先通过自己的手机(3)将自己的个人信用数据库帐户对应的状态标志设置为“开锁”状态，认让查看者在该“开锁”状态期间查看该受保护共享数据，而在查看者查看该受保护共享数据后，帐户保安系统(1)更可将查看者的身份和所查看过的受保护共享数据的简要，通过发短信给用户的手机(3)通知用户，既可保障用户的个人私隐不会被完全公开，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查看者查看。

[0028] 继续参阅图2，图2示出的方法还包括云计算系统(2)向帐户保安系统(1)查询某一帐户对应的状态标志的状态后，帐户保安系统(1)通过电话网络(4)发短信给该帐户对应的用户手机(3)，通知用户有关该次的查询。

[0029] 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)监控对帐户进行受监控操作的步骤，具体的步骤如下：

[0030] 1. 用户使用云设备(5)连线到云计算系统(2)，对该用户的帐户进行受监控操作前，用户使用手机(3)致电帐户保安系统(1)，拨通后就可立即挂线；

[0031] 帐户保安系统(1)从来电的电话号码找出对应该电话号码的状态标志，然后将该状态标志设置为“开锁”状态一段指定时间(例如指定时间为5分钟)，并在该段指定时间过后自动将该状态标志设置为“上锁”状态；

[0032] 2. 用户在该段指定时间期间，使用云设备(5)向云计算系统(2)发出要求对该用户的帐户进行受监控操作，云计算系统(2)收到该要求后向帐户保安系统(1)查询该帐户对应的状态标志的状态；

[0033] 3. 帐户保安系统(1)找出该帐户对应的状态标志的状态，由于用户是在该段指定时间期间发出该请求，所以状态标志处于“开锁”状态，帐户保安系统(1)将该“开锁”状态信息传送给云计算系统(2)，然后帐户保安系统(1)将该状态标志设置为“上锁”状态，以及，云计算系统(2)收到该“开锁”状态信息后允许进行该次受监控操作；

[0034] 4. 帐户保安系统(1)发短信给用户的手机(3)通知用户该帐户进行了一次受监控操作。

[0035] 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。

[0036] 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。

[0037] 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。

[0038] 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。

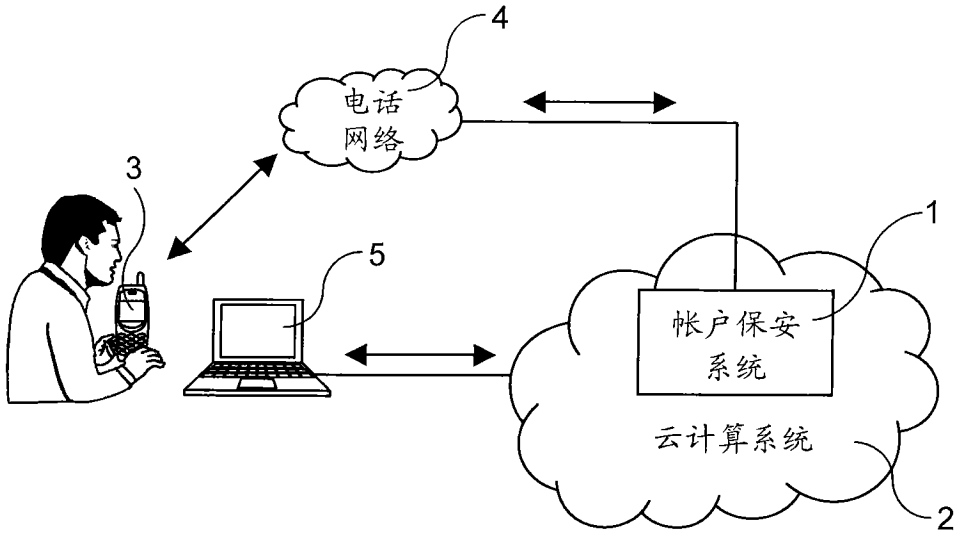


图 1

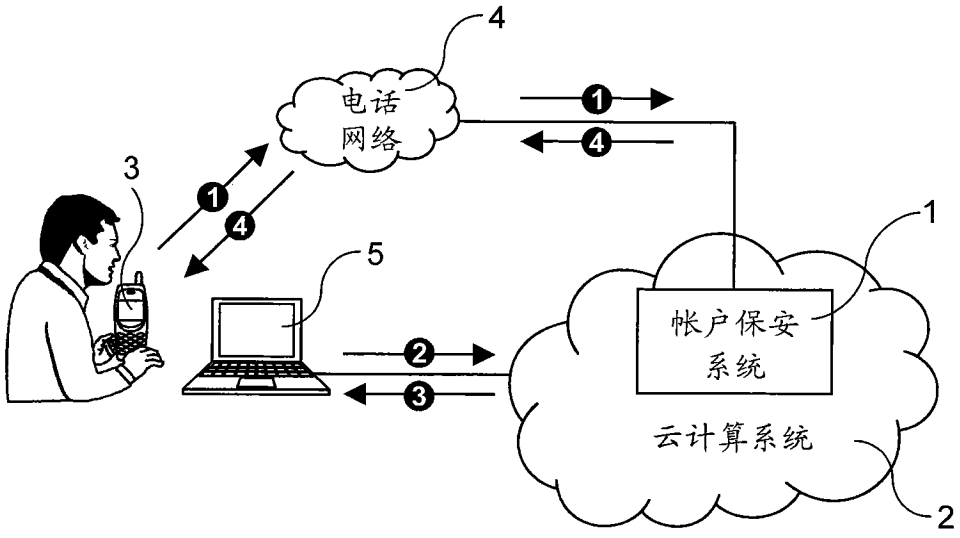


图 2