



(12) 发明专利申请

(10) 申请公布号 CN 102473210 A

(43) 申请公布日 2012. 05. 23

(21) 申请号 201080029844. 9

(22) 申请日 2010. 06. 29

(30) 优先权数据

1543/MUM/2009 2009. 07. 01 IN

(85) PCT申请进入国家阶段日

2011. 12. 30

(86) PCT申请的申请数据

PCT/IB2010/052959 2010. 06. 29

(87) PCT申请的公布数据

W02011/001371 EN 2011. 01. 06

(71) 申请人 芒达·帕蒂尔

地址 印度马哈拉施特拉邦

(72) 发明人 芒达·帕蒂尔

(74) 专利代理机构 北京华夏正合知识产权代理

事务所(普通合伙) 11017

代理人 韩登营

(51) Int. Cl.

G06F 21/00 (2006. 01)

权利要求书 3 页 说明书 8 页 附图 11 页

(54) 发明名称

远程控制及监视桌面软件数据的方法

(57) 摘要

本发明提供了一种利用 ISO 数据系统控制由软件生成的数据并防止该数据被非法使用的方法,其中,只能在建立该数据的电脑上使用或访问该数据。若要在其他电脑上使用该数据,则必须提供由数据所有者提供的使用或访问权限。

1. 一种方法,其特征在于,利用 ISO 数据系统控制由软件生成的数据并防止该数据被非法使用。

2. 根据权利要求 1 所述的方法,其特征在于,只能在利用 ISO 数据系统的电脑上才能使用由该电脑所创建的该数据;为了在其他电脑上使用该数据,数据所有者必须为在其他电脑上使用相同 ISO 数据系统的接受者授予权限。

3. 根据权利要求 1 所述的方法,其特征在于,包括:

选择待共享的数据,并将所有者 ID 嵌入到该数据中;

通过输入被允许共享数据的接受者的用户 ID 识别所述接受者,并授予至少一个所述接受者使用权限;

通过由所述数据所有者系统生成的唯一的数据 ID 识别共享的每组数据,其中每组数据的访问权限与每个特定的数据 ID 相关;

为授权接受者分配必要的访问权限以使用所述数据;

使用适当的数据共享方法,即通过向在线服务器上传数据实现共享或将数据拷贝到任意外部存储装置中。

4. 根据权利要求 1 所述的方法,其特征在于,在激活软件过程中,服务商在线服务器向所述软件发送两个密钥,即密钥 R1、R2;

密钥 R1 用于加密所有者的数据以防止该数据在其他电脑上被非法使用;当在所述软件中建立该数据时,自动以密钥 R1 加密该数据并将该数据以加密形式存储;

密钥 R2 用于在一个或多个预定接受者电脑系统上保护与所述预定接受者共享的数据;

Ra、Rb 分别为接受者的私钥和公钥。

5. 根据权利要求 3 所述的方法,其特征在于,所述数据所有者通过将所述数据上传至所述在线服务器,或通过所述数据转移至外部存储装置中并与接受者共享该外部存储装置,实现与所述接受者的数据共享。

6. 根据权利要求 3 所述的方法,其特征在于,如果所述接受者还未注册所述数据所有者的 R2 密钥,而需要将待共享数据上传至所述在线服务器,则首先使用所述数据所有者的 R1 密钥解密该数据,然后使用所述数据所有者的 R2 密钥加密该数据;之后,将待共享数据上传至所述在线服务器,并于所述在线服务器中使用所述数据所有者的 R2 密钥解密该数据,然后使用所述接受者的 Rb 密钥再次加密该数据;所述接受者下载该数据,并利用其 Rb 密钥使用该数据。

7. 根据权利要求 3 所述的方法,其特征在于,如果所述接受者还未注册所述数据所有者的 R2 密钥,而需要通过外部存储装置将待共享数据发送给所述接受者,则首先使用所述数据所有者的 R1 密钥解密该数据,然后使用所述数据所有者的 R2 密钥加密该数据;之后,将该数据转移至所述外部存储装置,与所述接受者共享该数据;

所述接受者将该数据上传至所述在线服务器,而如果所述数据所有者提供了充分的权限,所述在线服务器使用所述数据所有者的 R2 密钥解密该数据,并使用所述接受者的 Rb 加密该数据;之后,所述接受者下载该数据,并利用其 Rb 密钥使用该数据。

8. 根据权利要求 3 所述的方法,其特征在于,如果所述接受者在先注册了所述数据所有者的 R2 密钥,且需要将待共享数据上传至所述在线服务器,则首先使用所述数据所有者

的 R1 密钥解密该数据,然后使用所述数据所有者的 R2 密钥加密该数据;之后,将该数据上传至所述在线服务器,所述接受者从所述在线服务器上下载该数据,并利用所述数据所有者的 R2 密钥使用该数据。

9. 根据权利要求 3 所述的方法,其特征在于,如果所述接受者先注册了所述数据所有者的 R2 密钥,且需要通过外部存储装置共享该数据,则首先使用所述数据所有者的 R1 密钥解密该数据,然后使用所述数据所有者的 R2 密钥加密该数据;之后,将该数据转移至所述外部存储装置,与所述接受者共享该数据;所述接受者从所述外部存储装置上下载该数据,并利用所述数据所有者的 R2 密钥将该数据解密后使用该数据。

10. 根据权利要求 1 所述的方法,其特征在于,所述 ISO 数据系统用于保护所述数据所有者电脑或系统上的任何数据。

11. 根据权利要求 3 所述的方法,其特征在于,由授权和指定接受者下载的数据受到所述数据所有者分配的一定访问权限的限制;所述接受者只能根据访问权限的设置来使用所述数据;设置的所述访问权限为查看、修改、打印和保存。

12. 根据权利要求 3 所述的方法,其特征在于,授权的接受者修改所述数据;如果需要的话,将修改过的数据返回给所述数据所有者;使用新的数据 ID 识别修改过的数据;利用 Rb 密钥加密该修改过的数据,然后将其上传至所述在线服务器,在所述在线服务器上利用所述 Rb 密钥解密该数据,然后利用所述数据所有者的 R2 密钥再次加密该数据;之后,所述数据所有者下载该数据,将其转换回由 R1 密钥加密,并使用该数据。

13. 根据权利要求 12 所述的方法,其特征在于,所述接受者修改与所述数据所有者共享的数据;如果需要的话,通过将修改过的数据上传至在线服务器或将修改过的数据转移至外部存储装置后与所述数据所有者共享该外部存储装置,将该修改过的数据返回给所述数据所有者。

14. 根据权利要求 12 所述的方法,其特征在于,如果所述接受者还未注册所述数据所有者的 R2 密钥,利用所述接受者的 Rb 密钥加密经修改的待共享数据后将该数据上传至所述在线服务器,在所述在线服务器上利用所述数据接受者的 Rb 密钥解密该数据,然后利用所述数据所有者的 R2 密钥加密该数据;所述数据所有者下载该数据,将其由 R2 密钥加密转换回由其 R1 密钥加密,并使用该数据。

15. 根据权利要求 14 所述的方法,其特征在于,如果所述接受者还未注册所述数据所有者的 R2 密钥,而需要将修改过的待共享数据通过外部存储装置发送给所述数据所有者,则利用所述接收者的 Rb 密钥加密该数据后将该数据转移至所述外部存储装置,与所述数据所有者共享该数据;所述数据所有者将该数据上传至所述在线服务器,如果所述接受者提供了充分的权限,则所述在线服务器利用所述接受者的 Rb 密钥解密该数据,然后利用所述数据所有者的 R2 密钥加密该数据;之后,所述数据所有者下载该数据,将其由 R2 密钥加密转换回由 R1 密钥加密,并使用该数据。

16. 根据权利要求 12 所述的方法,其特征在于,如果所述接收者已在先注册了所述数据所有者的 R2 密钥,并将待共享的数据上传至所述在线服务器,则所述数据所有者下载该数据,利用其 R2 密钥解密该数据;之后,所述数据所有者将该数据由 R2 密钥加密转换回由 R1 密钥加密,并使用该数据。

17. 根据权利要求 12 所述的方法,其特征在于,如果所述接收者已在先注册了所述数

据所有者的 R2 密钥,并通过外部存储装置共享修改过的数据,则所述数据所有者从该外部存储装置中下载所述修改过的数据,并利用其 R2 密钥解密该数据;之后,所述数据所有者将该数据由 R2 密钥加密转换回由 R1 密钥加密,并使用该数据。

18. 根据权利要求 3 所述的方法,其特征在于,通过两种不同且互不相容的子系统处理原始数据及共享数据的存储和加工,并且所述原始数据及共享数据被分别存储在同一电脑或系统中两个分开的位置上。

19. 根据权利要求 12 所述的方法,其特征在于,提醒所述数据所有者,授权的接受者已修改了共享数据;如果需要的话,将修改过的共享数据与原始数据合并在一起。

20. 根据权利要求 1 所述的方法,其特征在于,为了保证数据共享的安全性,所述数据所有者通过发送注册 R2 密钥的指令给在线服务器并输入其他接受者及其本身的用户 ID,向其他接受者注册其 R2 密钥;任意一方通过向所述在线服务器发送撤销所述 R2 密钥注册的指令,可在任何时间撤销所述 R2 密钥的注册。

21. 根据权利要求 3 所述的方法,其特征在于,所述数据所有者通过通知所述在线服务器限制或删除发送给所述接受者的数据来限制与所述接受者共享的数据的访问权限。

22. 根据权利要求 3 所述的方法,其特征在于,即使来自于所述接受者电脑的数据存在于其他电脑上,由于缺少所述数据所有者的授权,也无法其他电脑上访问、使用或处理该数据。

23. 根据权利要求 1 所述的方法,其特征在于,如果需要重新安装所述软件,为软件用户提供了一种简易的重现安装方法,在所述软件激活后,在线服务器将加密、解密密钥发送给所述软件,还将其他用户在先注册的 R2 密钥发送给所述软件。

24. 根据权利要求 16 所述的方法,其特征在于,如果在重新安装软件过程中或每次开启软件时,检查出电脑的主板 ID 有变化,则需要重新向所述在线服务器确认所述软件,并需要由所述数据所有者使所述 R2 密钥重新生效,直到来自所述数据所有者的数据实现共享。

25. 根据权利要求 1 所述的方法,其特征在于,将所述 ISO 数据系统当做独立的加密模块使用,以确保数据存储的安全。

远程控制及监视桌面软件数据的方法

[0001] 芒达·马杜卡·帕蒂尔

[0002] 国籍:印度

[0003] 地址:印度马哈拉施特拉邦普纳阿恩德国民社会 85 号小区 118-124 号

[0004] 下列说明书特别描述了本发明及本发明的实施方式。

技术领域

[0005] 本发明涉及一种通过使用称之为 ISO 数据系统的方法,该方法避免软件数据被非法使用,ISO 数据系统提供了保护软件数据的保护机制。

[0006] ISO 数据系统特别是一种方法,使用 ISO 数据系统建立的数据对于安装在某一特定电脑上的软件是唯一且专有的。只能在建立该数据的电脑上使用该数据。若要在其他电脑上使用该数据,则必须提供由数据所有者提供的使用权限。

背景技术

[0007] 通常来讲,数据的本质是机密的。数据滥用会产生严重的损失,因此对于数据的保护是十分重要的。数据保护由三个主要部分组成,机密性、完整性以及可访问性。机密性是指防止数据被非法使用;完整性是指对于数据的修改只能在数据所有者的适当权限和授权下进行;可访问性简单来说是指需要使用数据时,数据必须可用。

[0008] 现有可用的保证数据安全的手段为使用密码、硬件锁定、数据加密等类似手段。

[0009] 在先技术:

[0010] 申请号为 20090259512 的美国专利记载了一种控制访问存储有大量媒体对象的媒体存储装置的方法,其中该方法包括接收用于识别所述媒体存储装置的第一数据,以及用于识别包含至少一个所述媒体存储装置的授权使用者的列表的第二数据;存储与第二数据相关的第一数据;为所述列表中的至少一个用户分配所述媒体存储装置;使用一传输会话标识符建立被分配的媒体存储装置与相当于与第二数据相关的使用者的用户识别系统之间的会话;然后根据从所述用户识别系统接收到的数据和所述传输会话标识符更新所述第二数据,由此修改所述被分配的媒体存储装置的授权列表。

[0011] 此外,上述文献还提供了一种用于控制媒体存储装置访问的分布式访问控制系统。该媒体存储装置存储有大量媒体对象。所述分布式访问控制系统包括接口,该接口用于接收识别所述媒体存储装置的第一数据和识别包含至少一个所述媒体存储装置的授权使用者的列表的第二数据;存储系统,用于存储与所述第二数据相关的所述第一数据;以及装置分配系统,用于为所述列表中的至少一个使用者分配媒体存储装置。所述装置分配系统用于建立传输会话标识符以为所述被分配的媒体存储装置与相当于与第二数据相关的使用者的用户识别系统建立一个传输会话。所述存储系统用于根据所述传输会话和从所述用户识别系统接收到的数据更新所述第二数据,由此修改所述被分配的媒体存储装置的授权用户列表。

发明内容

[0012] 本发明目的：

[0013] 数据滥用是指非法访问和使用数据。当数据对于非法用户为不可使用时，数据才是安全的，不会有问题。现有系统没有周全的、简单有效的方法来保护数据。有鉴于此，本发明的主要目的在于提供一种简单有效的方法来保护数据不被非法用户访问和使用。即便数据被非法获取，也不能被使用和处理。在一特定电脑上创建的数据不能在其他电脑上使用，除非数据所有者为其指定的每台可以共享该数据的电脑授予所需的权限。本发明还提供了一种自动操作的、简单且没有任何麻烦的用户软件重装系统。

[0014] 为了使用 ISO 数据系统，必须在服务商在线服务器上进行软件注册，因为只有软件注册用户才能使用该系统。软件注册系统及 ISO 数据系统为保证数据安全而紧密相关。在服务商在线服务器上成功注册软件后，一个唯一的、永久的用户 ID 被分配给每个注册软件。这个用户 ID 是唯一且重要的，用于识别安装于特定电脑上的特定软件的用户。在激活该软件的过程中，由所述服务器生成一个文件。该文件被发送给所述软件。这一文件对于用户而言是未知的，且包含密钥 R1 和 R2。所述服务器生成这些密钥并将这些密钥永久保存。这些密钥的功能是保护软件数据不被非法使用。这些密钥用于在必要过程中的加解密。R1 和 R2 都是永久密钥，其对于每个注册软件而言都是唯一的，并且与一个同服务商在线服务器和独一无二的安装软件有关的特定的唯一用户 ID 相关。密钥 R1 用于保护安装于软件所安装的特定电脑中的数据所有者的数据。R1 密钥不能与其他用户共享。默认下，总是由 R1 密钥加密由特定软件产生的数据，并将其一起存储在该软件安装的电脑中。R1 密钥为私钥。R2 密钥可以提供给其他电脑上的其他用户，如果需要的话，R2 密钥带有所述所有者的权限，用来保护需要共享的所述数据。R2 为该软件的公钥。

[0015] Ra 和 Rb 分别为接受者的私钥和公钥。所述公钥和所述私钥是机密的，不能无目的的使用或共享。数据所有者可以根据其需要将其 R2 密钥提供给一些接受者。所有者需要经常发送数据给这些接受者。所述数据所有者会向所述服务器发送一个指令，以通过输入所述接受者的用户 ID 将其 R2 密钥提供给所述接受者。这一指令还包含有所述数据所有者的用户 ID。当所述接受者与所述在线服务器建立连接时，会显示一个提示，请求所述接受者接受所述数据所有者的 R2 密钥。是否接受该密钥完全取决于所述接受者。所述数据所有者可以在任何时间通过向所述服务器发送指令来取消向其他接受者提供其 R2 密钥。而所述服务器无需接受者的权限便可取消向特定接受者提供所述数据所有者的 R2 密钥。

[0016] 数据是在使用软件时建立的信息。可使用任意外部存储装置或将数据上传至服务商的服务器以供接受者下载，来共享软件数据。所有者可以设置全部或部分访问权限，例如查看、可读、打印、保存和修改。即便是与其他接受者共享数据之后，对于数据的控制仍然属于数据的所有者。被授权的接受者每次访问共享数据时，如果需要的话，在线服务会检查访问权限状态。仅当所述访问权限仍然有效时，接受者才能访问该数据，否则将警告接受者该数据访问权限不再有效。如果需要，数据所有者还可以向在线服务器发出指令以从被授权接受者的电脑中删除其共享的数据。通过两个不同且互不相容的、分别支持加密系统的子系统来进行原始数据以及共享数据的处理和存储，并且数据被分别存储在同一电脑或系统中两个分开的位置上。利用 ISO 数据系统可防止数据被非法使用。下面，进一步介绍利用 ISO 数据系统保证数据合法使用的方法。在本实施例中，系统环境包括数据所有者、数据所

有者需要与其共享数据的接受者以及在线服务器。数据所有者可与其他注册接受者共享数据。所述接受者可能具有或不具有所述数据所有者的、向所述接受者注册的 R2 密钥。在这两种情况下,可通过两种方法来共享数据,其中之一为通过向所述在线服务器上传共享的数据集/包,另一种为将共享数据拷贝到任意外部存储装置上,并与预订接受者共享这一装置。

[0017] 在接受者没有数据所有者的 R2 密钥的情况下,数据接受者将通过将数据上传至在线服务器来共享该数据。因为被共享的数据已由数据接受者的 R1 密钥加密,因此使用该 R1 密钥解密该数据,然后在每次由标准密码原理控制的数据接受者电脑上使用 R2 密钥加密该数据。

[0018] 而且,接受者的用户 ID 与发送者的一样被输入该数据。由数据所有者共享的每个数据集或包将包含一由数据所有者系统生成的特定数据 ID。所述数据 ID 将确定用于共享的每个数据集的唯一性,并起到管理所述数据的作用。每个数据集的访问权限及对应信息与其各自的数据 ID 关联。服务器将持续记录所有数据集/包以及与所有数据集/包的数据 ID 相关的所有属性。然后,将这一数据上传至在线服务器,在该服务器上使用数据所有者的 R2 密钥再次解密该数据并将该数据转换成普通/原始格式。之后,利用接受者的 Rb 密钥将其加密。现在服务器向接受者发送某数据待共享的提醒。最后由接受者下载该数据并使用数据接受者 Rb 密钥解密该数据。

[0019] 可以通过外部存储装置向接受者提供相同数据。在这种情况下,接受者将该数据上传至在线服务器。所述服务器将检查所述数据所有者是否已经为上传该数据的特定接受者的用户 ID 设置了权限,并且仅当设置有权限时,才处理该数据并将该数据发回给接受者。如果所述数据所有者没有授予权限,所述在线服务器则将该数据从接受者电脑中删除。在用户(接受者)向所述在线服务器上传该数据时发生的解密、加密如上述解密、加密过程,并且在用户连接到所述在线服务器时,其可以下载并使用该数据。在用户具有数据所有者的注册有该用户的 R2 密钥的情况下,所述数据所有者还可以通过将数据上传至在线服务器或通过将数据存储在外部存储装置上后与用户共享该外部存储装置来实现该数据的共享。在这种情况下,使用同一 R1 密钥来解密已加密的数据,并再次使用所述数据所有者的 R2 密钥来加密该数据。无论所述数据所有者采用何种方式将该数据发出,所述用户都可以从所述服务器处下载该数据或从所述外部存储装置中获得该数据。因为,所述用户已获得所述数据所有者的已注册的 R2 密钥,因此可使用所述数据所有者的 Rb 密钥解密该数据后使用该数据。

[0020] 即便该数据意外被具有所述数据所有者 R2 密钥的非法软件获取,由于想要打开该数据的非法软件的用户 ID 与合法的用户 ID 不同,因此利用该软件的用户 ID 不能访问该数据。

[0021] 只能以所述服务器的授权来使用所述共享数据,且该共享数据存储在与原始位置不同的位置上。所述接受者下载该数据后将其导入软件。根据赋予的数据访问权限来使用数据。访问权限有两种类型:一种为只能查看的访问权限,该权限只能查看数据不能保存数据;第二种为全部或部分使用或修改数据的访问权限。只能在由所述数据所有者设置的数据访问、使用权限下进行相关的数据操作。举例来说,可以使用 x 天、x 小时、x 次所述数据,或者允许或不允许修改、保存或打印所述数据。

[0022] 如果接受者修改了数据并想与数据所有者共享该经修改的数据,则有四种方式可实现这一目的:方式 1,如果所述接受者没有所述数据所有者的 R2 密钥,所述接受者可使用其 Rb 密钥加密所述数据后返回给所述所有者。其中,可通过两种方法将所述数据返回给所述数据接受者:一种为所述接受者将该数据上传至在线服务器,由在线服务器将使用 Rb 密钥加密的所述数据转换为使用所述数据所有者的 R2 密钥加密的数据,并通过其与所述数据所有者之间连接将该数据发送给所述数据所有者。所述数据所有者下载该数据,并使用 R1 密钥解密由 R2 密钥加密的数据,以便使用该数据。所述接受者可以采用的第二种为将使用 Rb 密钥加密的待共享数据存储在外部存储装置中。在这种情况下,所述数据所有者从该外部存储装置中获得所述数据,并将该数据上传至在线服务器,由在线服务器将使用 Rb 密钥加密的所述数据转换为使用 R2 密钥加密的数据后,再由所述数据所有者下载该数据并使用 R1 密钥解密由 R2 密钥加密的所述数据,以便使用该数据。

[0023] 方式 2,如果所述接受者具有所述数据所有者的 R2 密钥。在这种方式下,所述接受者仍然可以通过外部存储装置或上传数据至在线服务器将经修改的数据返回给所述数据所有者。在这两种情况下,使用数据所有者的 R2 密钥加密该数据后发送该数据。不管接受者使用何种方法将该数据发出,数据所有者可以通过在线服务器下载该数据或从外部存储装置中获取该数据,并使用 R1 密钥解密由 R2 密钥加密的所述数据,以便使用该数据。

[0024] 对于数据的修改会显示给数据所有者,并仅当数据所有者接受修改时,才可导入、合并该数据。为所述数据所有者提供可以合并由所述接受者修改过的数据的能力。将修改过的待共享数据保存在与软件原始位置不同的位置上,除非有指令要求,否则待共享数据与接受者软件的原始数据/记录互不干扰。如果接受者需要修改该数据,那么在合并或集成接受者的修改之前,所述数据所有者可以保存该数据的原始拷贝。如果数据所有者想同多个接受者共享数据,则可以使用相同的方法来实现这一目的。

[0025] 在接受者想要重新安装该软件的情况下,将打开一重新安装向导。该向导获取用户 email ID 输入。完成验证后,从服务器获取账号信息并完成所述软件的重新安装。所述服务器会发送一个用户注册 email ID 确认密钥。该确认密钥仅在一次事务处理中有效,并与该软件的激活文件相关。当激活文件从所述服务器发送至该软件之后,由用户将注册 email ID 确认密钥输入至软件激活向导。如果在注册软件时,所述电脑的主板 ID 与在线服务器上注册的主板 ID 相匹配,则由所述服务器在该软件中恢复所述密钥 R1、R2。该软件接受者会向其他接受者发出请求,请求其他接受者重新向该软件注册其各自的 R2 密钥。如果在重新安装过程中,电脑的主板 ID 与在线服务器上注册的主板 ID 不匹配,则将重新安装该软件,但由于主板 ID 差异不会再次注册先前向所述服务器注册的 R2 密钥,并且该软件会提醒接受者向不同数据所有者再次发送要求,要求不同的数据所有者重新向该软件注册其各自的 R2 密钥。

[0026] 每次打开软件时,授权组件将嵌入该软件的主板 ID 与电脑主板的 ID 进行匹配。如果主板 ID 不匹配,则阻止使用该软件并提醒接受者需要去在线服务器验证。一旦接受者通过在线服务器验证,会向用户注册 email ID 发送一确认密钥,之后将密钥 R1、R2 发送并恢复至该软件。该软件仍然会提醒接受者再次向不同数据所有者发送要求,要求不同的数据所有者重新向该软件注册其各自的 R2 密钥。只有在数据所有者确认后,才再次向接受者注册他们各自的 R2 密钥。每次电脑与网络连接时,所述服务器会检查向所述软件注册的 R2

密钥的状态。如果所述服务器发现一特定数据所有者的 R2 密钥已被取消,则所述服务器将取消以该 R2 密钥注册的接受者。同样地,所述接受者也可以通知所述服务器取消一特定 R2 密钥的注册。在这种情况下,将提醒所述数据所有者,其 R2 密钥未被一特定接受者注册。

[0027] 有益效果及应用:

[0028] 本发明方法 ISO 数据系统可以帮助软件所有者保护其软件数据不受非法访问。所述软件所有者可以设置接受者的数据使用限制条件。可通过外部装置或将其上传至在线服务器来实现数据共享。

[0029] 鉴于在本发明思想下的不同实施方式,不难理解这些经阐明的实施方式仅为本发明的较佳实施例而已,并不用以限制本发明。凡在本发明的精神和原则之内,所作的任何修改、等同替换、改进等,均应包含在本发明的保护范围之内。

附图说明

[0030] 图 1a、1b 为所有者注册软件和使用数据的方法流程图;

[0031] 图 2a、2b 为实现数据在线共享的方法流程图;

[0032] 图 3a、3b 为使用诸如硬盘实现数据共享的方法流程图;

[0033] 图 4a、4b 为重新安装、分配密钥的方法流程图;

[0034] 图 5 为与不同潜在接受者共享 R2 密钥的方法流程图;

[0035] 图 6 为取消潜在接受者使用 R2 密钥的方法流程图;

[0036] 图 7 为授权的方法流程图。

具体实施方式

[0037] 所述 ISO 数据系统程序是一种写入 Microsoft .NET 编程语言中的字节码程序。

[0038] 说明书中提供了一种避免用户数据被非法访问的方法。将用户注册于在线服务器上的方法包括接受一预期用户对于桌面软件的初始访问,并确认该用户是否已经提供有效的用户识别信息。如图 1a 所示,用户执行功能 101 以在其电脑上安装软件,在软件安装成功的基础上,用户准备开始使用软件。用户点击该软件以第一次使用该软件,由此执行了方法 102。当所有者第一次使用该软件时,执行方法 103 从该桌面软件中弹出软件注册窗口以完成用户于服务商在线服务器上的注册。在方法 104 中,所述所有者在由方法 103 产生的所述注册向导中输入注册信息。如果网络连接可用,则方法 105 验证了与每个载入对象有关的方法 105 的完整性。如果成功执行了方法 106,则方法 107 在成功调用方法 108 的基础上验证用户信息。通过执行方法 109 于所述服务商在线服务器上注册用户,并由所述服务器向所述用户分配唯一的用户 ID,并通过执行方法 110 将该用户 ID 嵌入所述软件。执行方法 111 (如图 1b 所示) 以显示激活向导。用户选择认购选项,即试用或认购,然后执行方法 112 将确认密钥发送至用户注册 email ID。所有者在由执行功能 113 产生的激活向导中输入该确认密钥。所述软件执行网络连接可用类 114 以检查网络连接。如果网络可用,则功能 116 通过执行网络连接可用类 117,于在线数据库中验证所述确认密钥。在成功验证的基础上,方法 118 使所述服务器发送一带有加密用户 ID 的激活文件,这一激活文件还包含两个用于所述软件数据加解密的唯一密钥 R1、R2,安装 ID、由在线服务器授予用户电脑的数据使用周期,并将用户电脑主板 ID 存储至在线数据库。所述软件建立了一个以所有者 R1

密钥进行加密的数据库。

[0039] 如图 2a 所示,如果所述数据所有者想要通过方法 201 与其他注册接受者共享其数据,由于数据在建立时是以所述数据所有者的 R1 密钥进行初始加密的,因此使用所述数据所有者的 R1 密钥对所述软件数据进行解密。然后在所述数据所有者通过执行方法 202 输入用户 ID、输入密码后,使用所述数据所有者的 R2 密钥加密该数据。所述数据所有者设置该数据的访问权限,通过执行功能 203 由系统为该组数据分配唯一的数据 ID。执行方法 204,数据所有者需要选择数据共享的方式。如果数据所有者选择了通过执行方法 205 实现在线数据共享,且所述网络连接可用,则所述软件验证与每个载入对象相关的方法 206 的完整性,如果成功执行了所述方法 206,则执行方法 207 以检查所有者是否有接受者的 Rb 密钥:如果所有者有接受者的 Rb 密钥,则执行功能 208 使用 Rb 密钥加密所述数据并将该数据存储于在线服务器上。另外,执行方法 209 将所述数据与 R2 密钥一起存储于在线服务器上,在线服务器使用数据所有者的 R2 密钥解密该数据,并使用接受者的 Rb 密钥再次加密该数据。如果网络连接可用,则软件验证机制 210 验证与每个载入对象相关的方法 210 的完整性。如果所述方法 210 通过验证,则执行方法 211 以提醒接受者接收该数据。接受者通过执行方法 212 从所述服务器处下载所述数据所有者的数据。如果方法 214 通过验证,则执行方法 215(如图 2b 所示)以利用接受者的 Rb 密钥对该数据进行解密,并将该数据导入在另一位置上的接受者软件中。软件验证机制 216 验证数据共享权限:如果软件通过执行方法 217 且成功执行了方法 217 检查出接受者具有修改所述数据的权限,则执行方法 219 以根据权限设置修改所述数据;如果不具有修改所述数据的权限,则所述接受者只能通过方法 218 查看该数据。

[0040] 在完成对于所述数据的修改之后,功能 220 对于检查接受者是否拥有所述数据所有者的 R2 密钥进行验证:如果成功执行了功能 220,则执行方法 221 以利用所述所有者的 R2 密钥加密该数据,并将该数据上传至所述在线服务器。另外,通过执行方法 222 以接受者的 Rb 密钥加密经修改的数据,并将该数据上传回所述服务器。在所述服务器端,以接受者的 Rb 密钥解密该数据,并通过执行方法 223 以所述数据所有者的 R2 密钥再次加密该数据。之后,所述所有者由方法 225 获得被修改的数据的提醒。如果网络连接可用,则软件验证机制 224 验证与每个载入对象相关的方法 224 的完整性。如果成功执行方法 225 以提醒所述所有者,则执行方法 226 以下载该数据。该软件检查接受者是否为一个执行方法 227 的预定接受者:若是,验证机制 228 验证与每个载入对象相关的方法 228 的完整性:如果方法 228 成功通过验证,则由所述所有者执行方法 230 以将该数据导入在另一位置上的接受者软件中;否则,通过执行方法 229 丢弃该数据。如果所述所有者接受该数据,则通过执行方法 231、232 将该数据与原始数据合并。

[0041] 如图 3a 所示,如果数据所有者想通过执行方法 301 来与其他注册接受者共享其数据,因为在建立该数据时,是以所述数据所有者的 R1 密钥进行初始加密的,因此软件使用该 R1 密钥解密该数据,然后通过执行方法 302 使用 R2 密钥加密该数据。上述过程仅发生在所述数据所有者输入密码以执行这一事务处理之后。所述数据所有者设置修改所述数据的权限,并通过执行功能 303 将唯一的数据 ID 分配给该组数据。所述数据所有者通过方法 304 选择共享数据的方式,即通过在线的方式或通过外部存储驱动器的方式。如果所述数据所有者选择了通过执行方法 305 以通过外部存储驱动器实现数据共享的方式,则执行功能

306 以检查所述数据所有者是否有接受者的 Rb 密钥。如果所述数据所有者有接受者的 Rb 密钥,则执行功能 307 以使用 Rb 密钥加密该数据并将该数据存储于在线服务器上;否则,执行方法 308 以使用 R2 密钥和用户(接受者)信息加密该数据。所述数据所有者通过执行方法 309 以外部存储驱动器向接受者发送加密的数据。接受者通过执行方法 310 接受该数据。软件通过执行方法 311 交叉检查接受者的用户 ID 来检查接受者的合法性。软件检查机制 312 检查与每个载入对象相关的方法 312 的完整性,如果方法 312 通过检查,则执行方法 313(如图 3b 所示)以解密该数据并将该数据导入接受者的软件。检查机制 314 检查数据修改的权限设置,如果接受者具有通过执行方法 315 来修改数据的权限,且成功执行了方法 315,则通过执行方法 316 以与该接受者相关的 Ra 密钥界面数据,而其他接受者只能通过执行方法 317 来查看数据。因此,在完成对于该数据的修改之后,接受者根据由执行方法 316 而确定的权限设置来更新所有者的数据。功能 318 验证接受者是否有所有者 R2 密钥的检查;如果成功执行了功能 318,则通过执行方法 322 以所有者的 R2 密钥加密更新的数据。接受者通过执行功能 323 将该数据上传回外部存储驱动器,而所述数据所有者通过执行方法 324 从所述外部存储驱动器中获取所述更新数据。此外,软件还以接受者的 Rb 密钥加密该数据,并通过执行方法 319 将该数据上传回所述外部存储驱动器,而所述数据所有者通过执行方法 320 接收该数据并将该数据上传至所述在线服务器。最后,所述在线服务器利用 Rb 密钥加密该数据并利用 R2 密钥再次加密该数据后,通过执行方法 321 将该数据发送至所述所有者。软件通过执行方法 325 来检查所述接受者是否为预定接受者;若是,验证机制 326 验证与每个载入对象相关的方法 326 的完整性,如果成功执行了方法 326,则由所有者执行方法 328 以将该数据导入所述软件;否则,通过执行方法 327 丢弃该数据。如果所述所有者通过执行方法 329 接受了该数据,则执行方法 330 将该接受数据与所有者的原始数据合并。根据本方案,避免了对于给定数据的非法访问。

[0042] 如图 4a 所示,如果接受者由于一些原因需要重新安装所述软件,执行了方法 401。接受者通过执行功能 402 来重新安装所述软件。当接受者点击开启所述软件时,执行了方法 403,软件注册窗口 403 会弹出。通过执行功能 405,接受者输入注册的 email ID 和密码,然后点击“下一步”进行继续处理。如果网络连接可用,方法 406 验证与每一载入对象相关的方法 406 的整体性。如果成功验证了方法 407,则执行方法 408 以通过检索服务商在线服务器来验证输入的注册信息是否有效;如果注册信息是有效的,则方法 409 验证其与每个载入对象相关的完整性。如果成功验证了方法 409,则执行方法 410 以获取已在所述在线服务器上注册的接受者的所有信息。方法 411 重新安装所述软件并执行了方法 412(如图 4b 所示)以将确认密钥发送给用户注册 email ID,通过执行方法 413 输入确认密钥并点击“下一步”。软件通过检索所述在线数据库以验证所述确认密钥是否有效;如果通过执行方法 416 验证所述确认密钥有效,则通过执行功能 417 无效掉所有先前特定接受者的安装 ID,并生成新的、唯一的安装 ID 并将机器码存储于在线数据库。软件通过执行方法 418 以检查嵌入其中的主板 ID 是否与电脑主板 ID 相一致。验证机制 419 验证了主板 ID。通过执行功能 420 为接受者分配新的 R1、R2 密钥,并提醒接受者再次向不同的数据所有者发送重新向所述软件注册数据所有者各自 R2 密钥的请求。只有在数据所有者确认后,才能再次向所述接受者注册其 R2 密钥。

[0043] 如图 5 所示,如果所述数据所有者想要与其他注册接受者共享其 R2 密钥,则执行

方法 501。向导 502 弹出,以输入接受者的用户 ID。所述数据所有者通过执行功能 503 输入其欲与之共享数据的接受者的用户 ID。如果网络连接可用,验证机制 504 验证与每个载入对象相关的方法 505 的完整性。如果成功验证了方法 505,则执行方法 506 以将带有接受者用户 ID 的 R2 密钥存储在所述在线服务器上。如果网络连接可用,验证机制 507 验证其与每个载入对象相关的完整性。如果成功验证了方法 507,则执行方法 508 以提醒接受者注册该密钥。现在,如果接受者通过执行功能 509 接受该提醒以注册该密钥,如果网络连接可用,则验证机制 511 验证与每个载入对象相关的方法 511 的完整性;如果成功验证了方法 511,则通过执行方法 512 以提醒所述数据所有者向接受者注册 R2 密钥。如果接受者不接受方法 510,则无法注册该密钥。

[0044] 如图 6 所示,如果数据所有者想撤销与其他接受者共享 R2 密钥,则执行方法 601。显示出注册有数据所有者 R2 密钥的用户 ID 的列表的界面 602 弹出。数据所有者选出其要从中撤销其 R2 密钥的接受者的用户 ID,并通过执行功能 603 将这一请求发送至所述在线服务器。如果接受者电脑上的网络连接可用,则连接验证机制 604 验证与每个载入对象相关的方法 605 的完整性。如果成功验证了所述方法 605,则执行方法 606 以由在线服务器从预定接受者中撤销注册的 R2 密钥。如果所述数据所有者电脑上的网络连接可用,则连接验证机制 607 验证其与每个载入对象相关的完整性。如果成功验证了所述方法 607,则执行方法 608 以提醒所述数据所有者已成功从预定接受者中撤销了 R2 密钥。

[0045] 如图 7 所示,每当开启所述软件时,授权组件 701 检查嵌入软件的主板 ID 是否与电脑主板 ID 相符。功能 702 检查所述嵌入软件的主板 ID 是否被更改,若被更改则执行功能 703 屏蔽所述软件并提醒接受者去在线服务器验证。如果网络连接可用,则连接验证机制 704 验证与每个载入对象相关的方法 705 的完整性。如果成功验证了方法 705,则执行方法 706 以向所述在线服务器确认所述软件并将确认密钥发送至用户注册 email ID。接受者通过执行功能 707 将所述确认密钥输入至激活向导。如果验证机制 708 向所述在线服务器确认了该确认密钥,则执行功能 709 以向所述在线服务器注册新的主板 ID,并通过这一主板 ID 识别所述软件。执行功能 710 以向接受者发送并恢复 R1、R2 密钥。执行功能 711 以提醒所述数据所有者请求其他数据所有者向所述软件注册其各自的 R2 密钥。只有在数据所有者确认后,才能再次向接受者注册数据所有者的 R2 密钥。

图1 注册及密钥传递

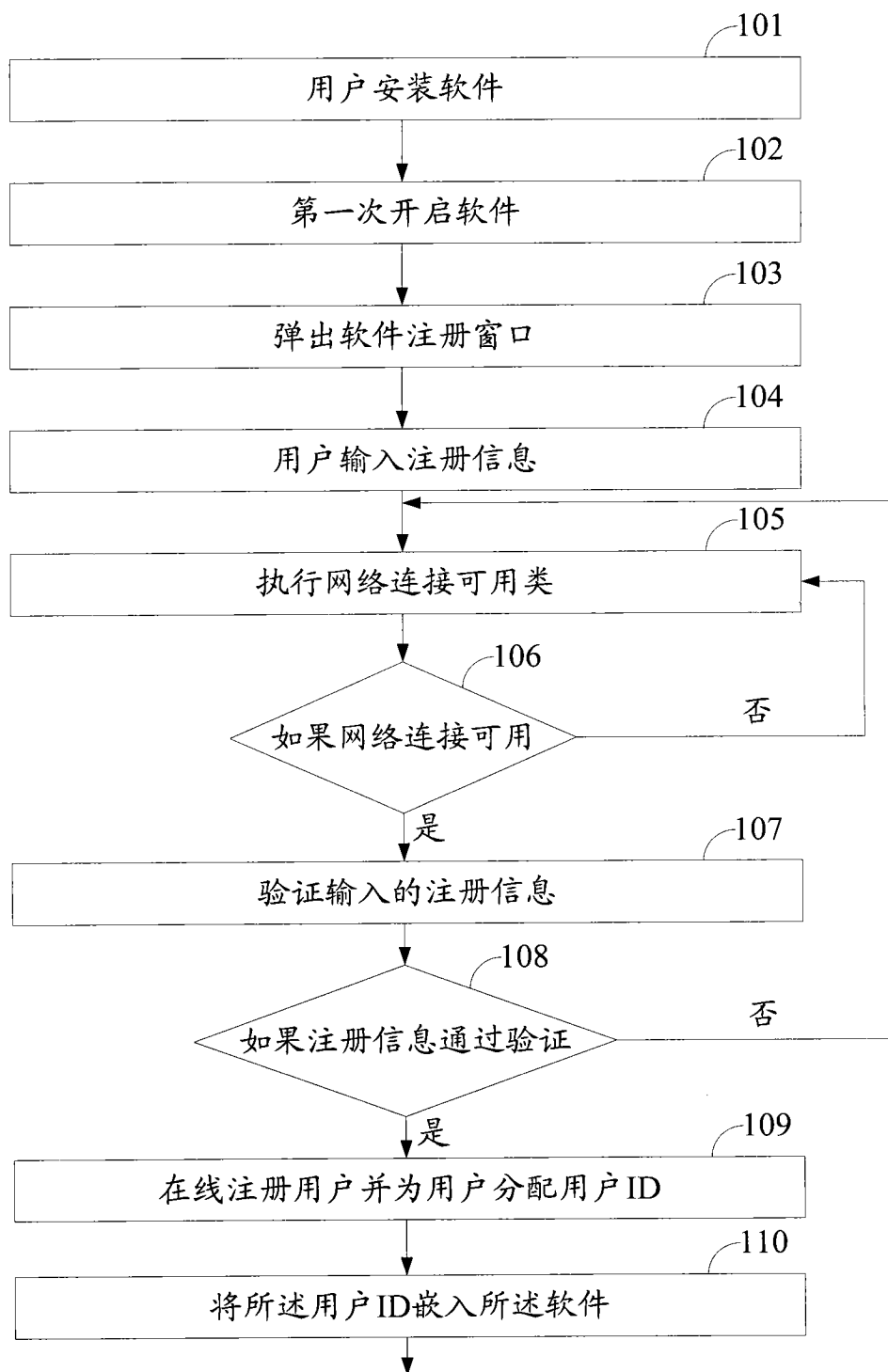


图 1a

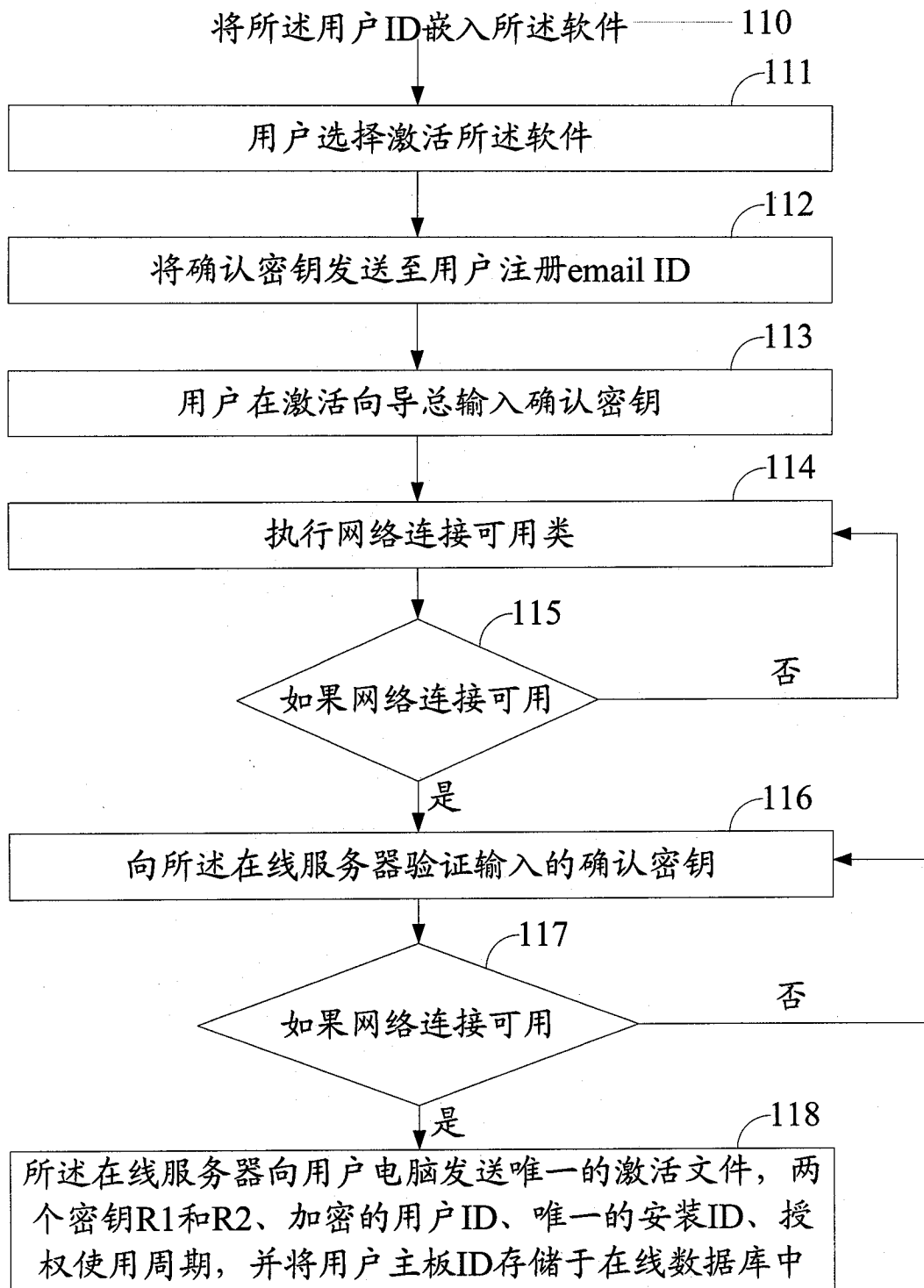


图 1b

图2 通过在线方式共享数据

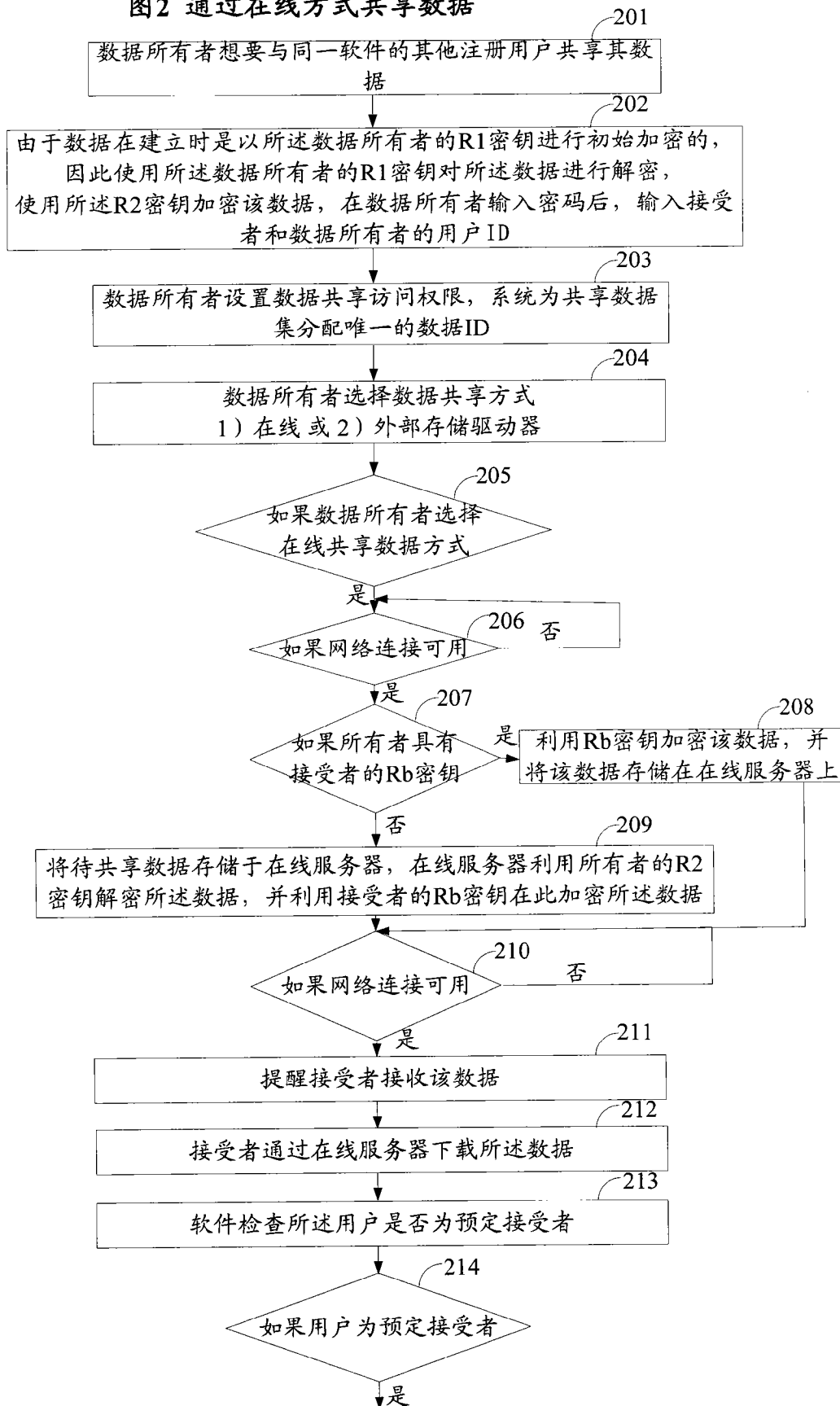


图 2a

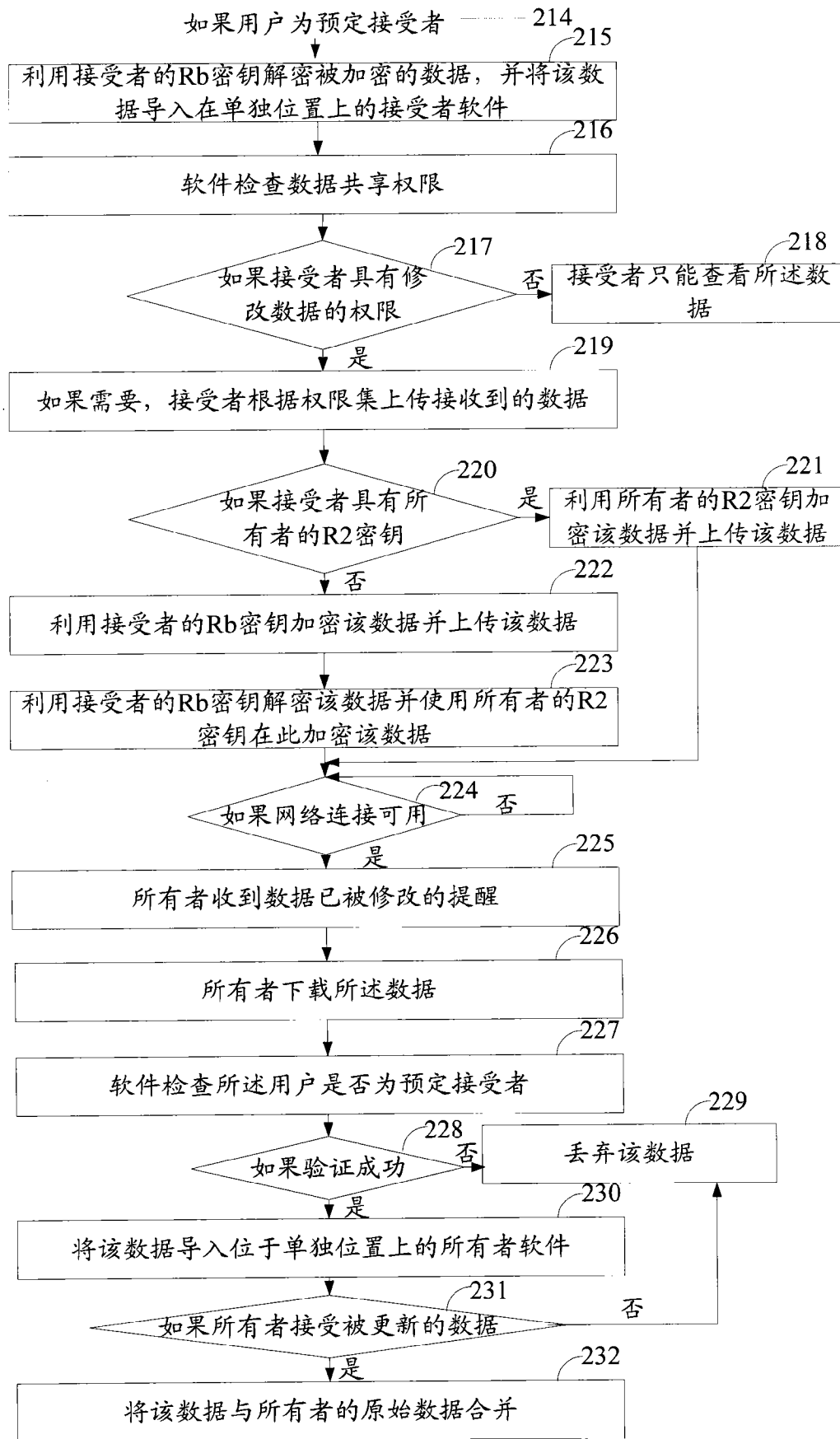


图 2b

图3 通过外部存储驱动器共享数据

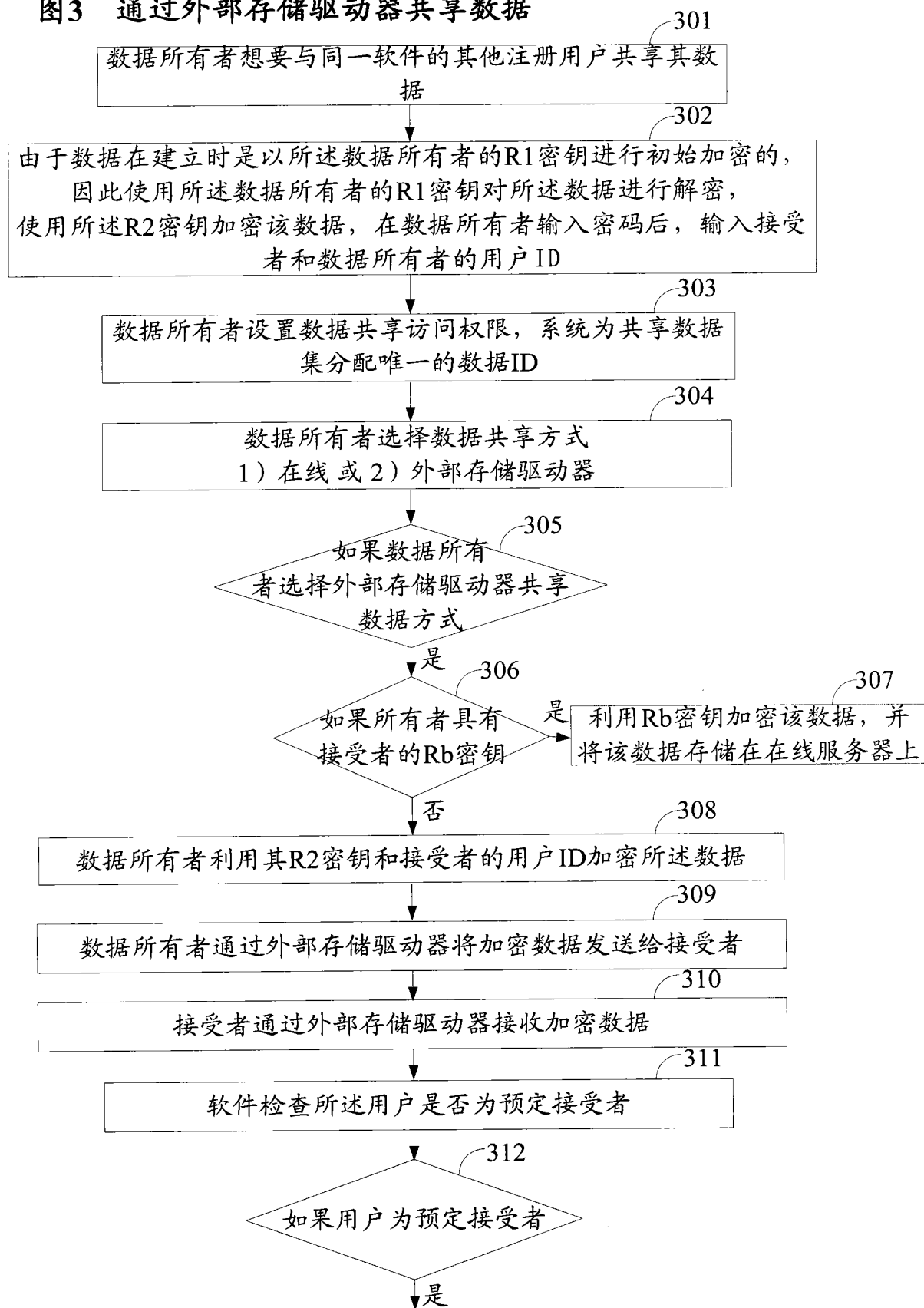


图 3a

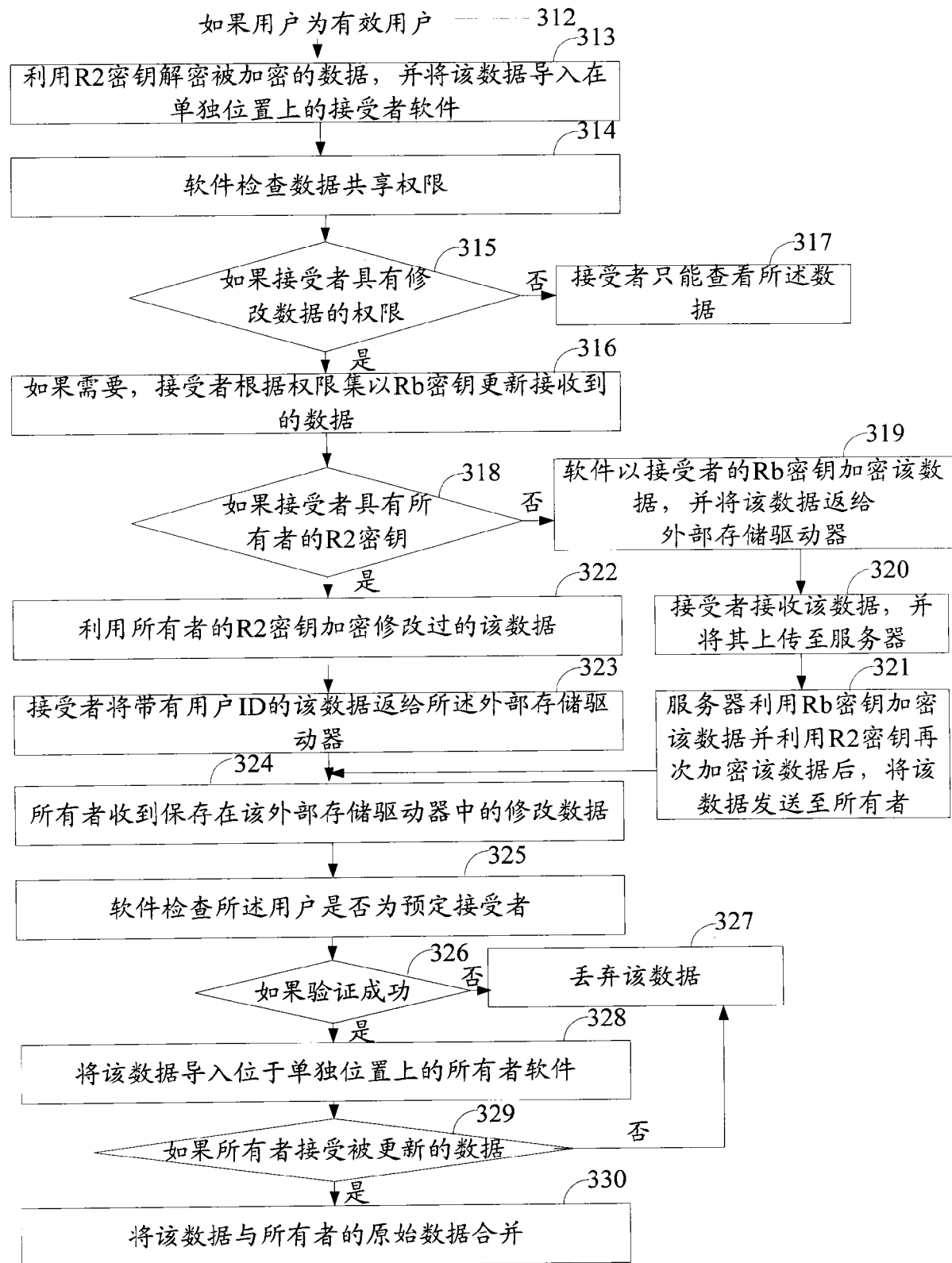


图 3b

图4 软件的重新安装及密钥的重新分配

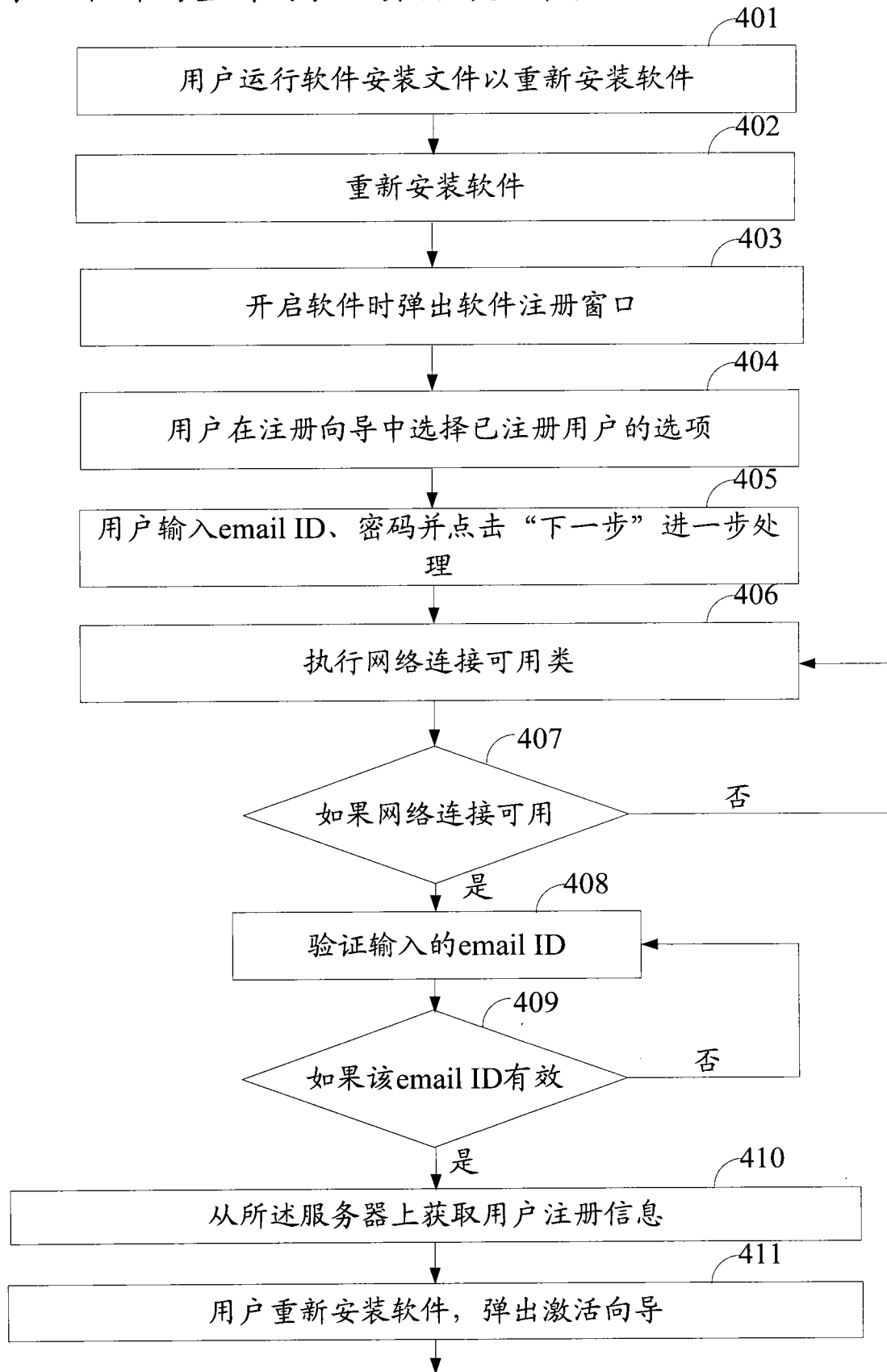


图 4a

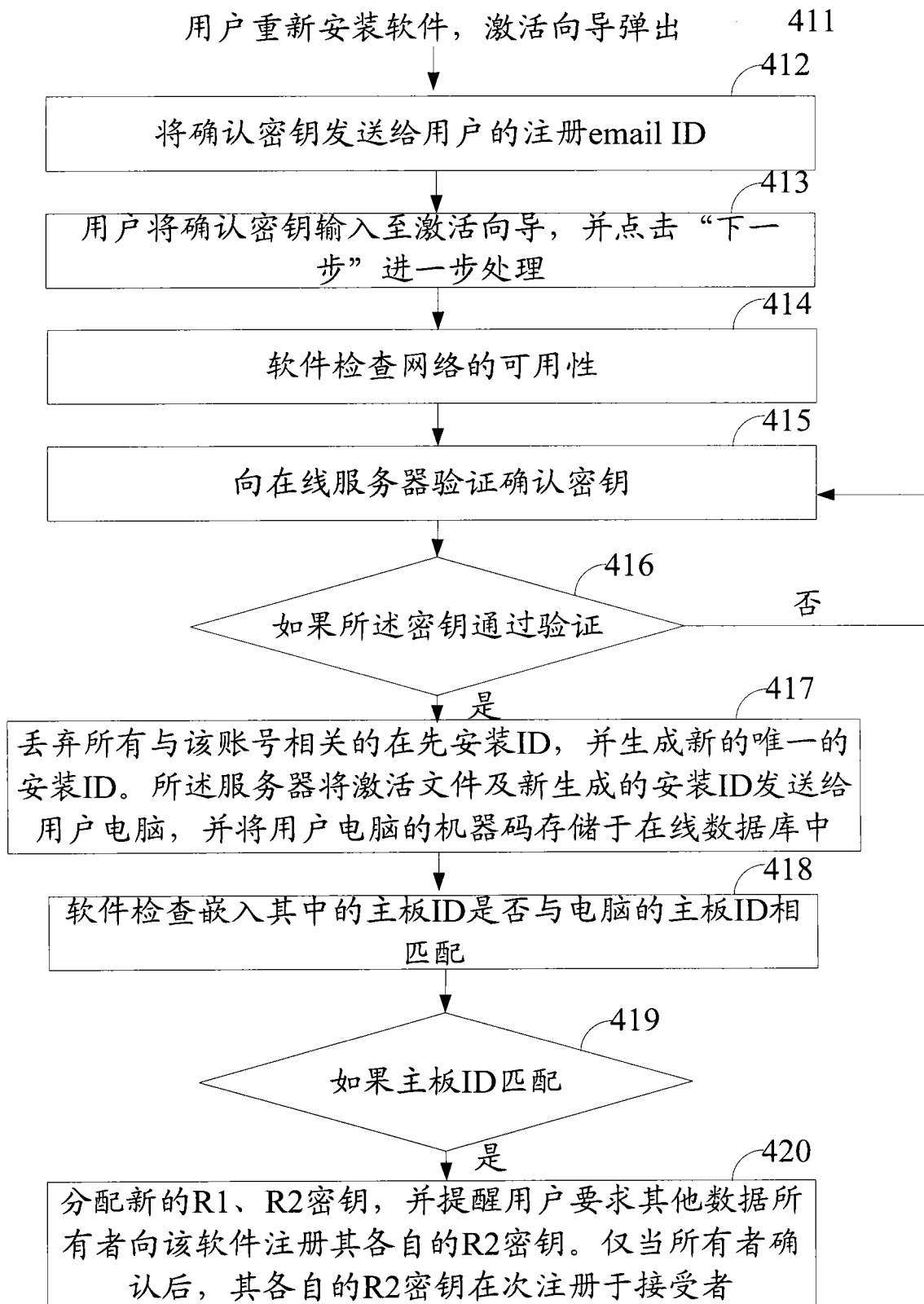


图 4b

与多用户共享密钥

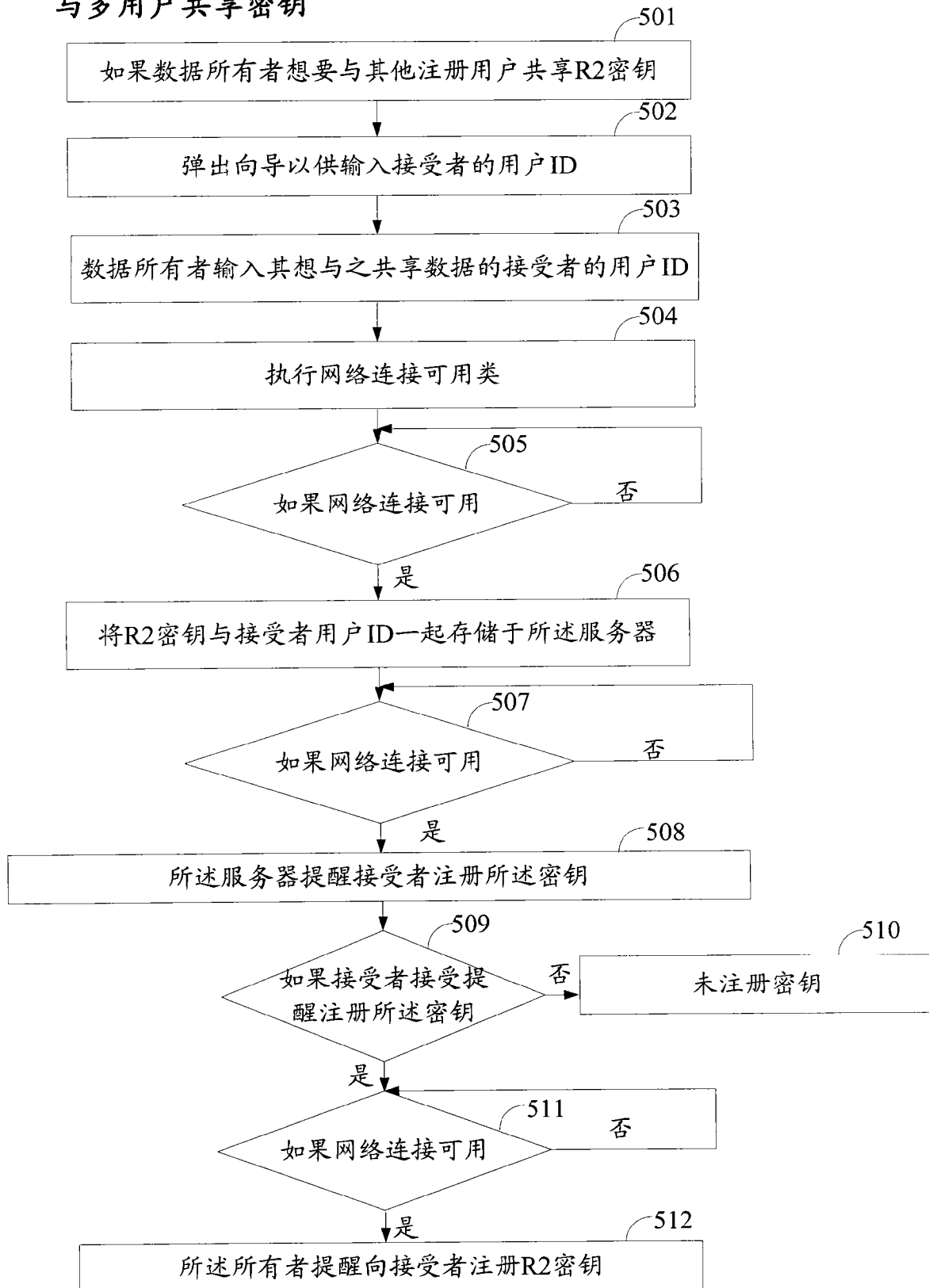


图 5

从接受者处撤销R2密钥

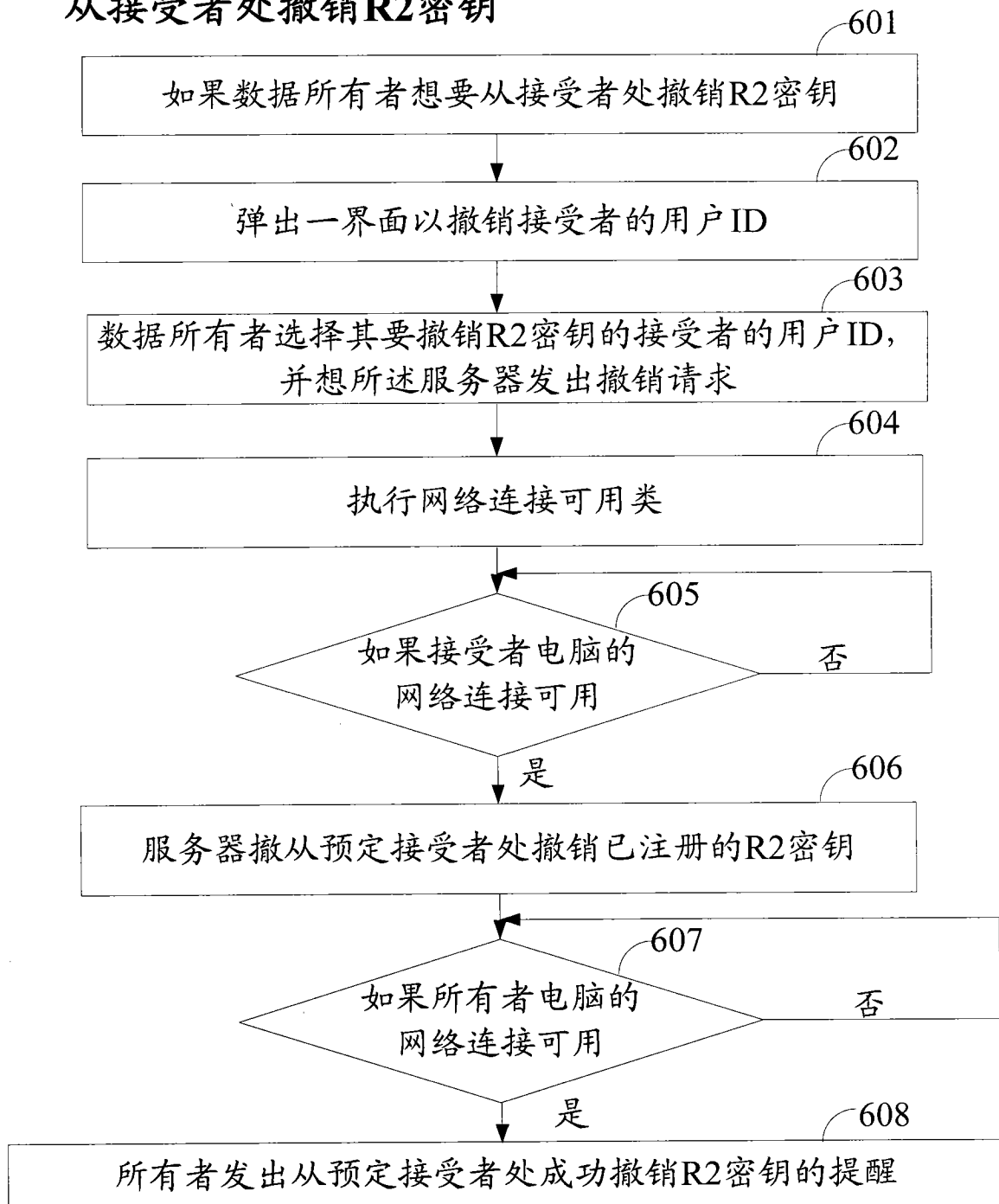


图 6

授权

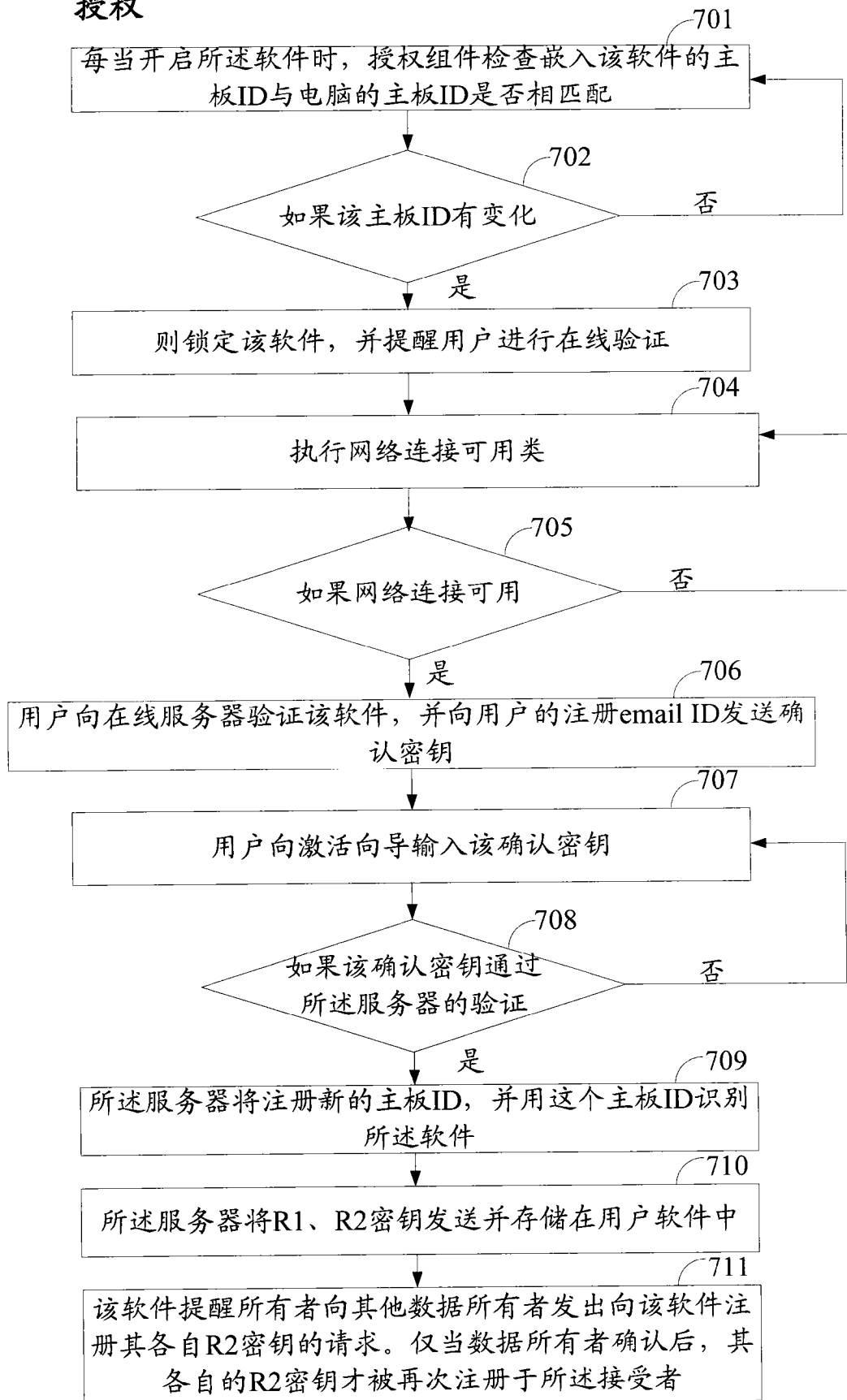


图7