(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 110431557 B
(45)授权公告日 2023.09.26

(21)申请号 201880006190.4

(22)申请日 2018.01.09

(65)同一申请的已公布的文献号
申请公布号 CN 110431557 A

(43)申请公布日 2019.11.08

(30)优先权数据
17305020.4 2017.01.09 EP

(85)PCT国际申请进入国家阶段日
2019.07.08

(86)PCT国际申请的申请数据
PCT/EP2018/050474 2018.01.09

(87)PCT国际申请的公布数据
WO2018/127606 EN 2018.07.12

(73)专利权人 交互数字麦迪逊专利控股公司
地址 法国巴黎

(72)发明人 大卫·马腾斯 奥利弗·阿杜安

(74)专利代理机构 中科专利商标代理有限责任公司 11021
专利代理师 潘剑颖

(51)Int.Cl.
G06F 21/62(2006.01)
G06F 11/14(2006.01)

(56)对比文件
CN 103631672 A,2014.03.12
US 2005228994 A1,2005.10.13
WO 2013179128 A1,2013.12.05
US 2014068258 A1,2014.03.06
CN 1476580 A,2004.02.18
US 2016350238 A1,2016.12.01
JP 2004259262 A,2004.09.16
CN 104025542 A,2014.09.03
CN 101006428 A,2007.07.25
US 2014149701 A1,2014.05.29
CN 101536007 A,2009.09.16
CN 101400060 A,2009.04.01
CN 102915263 A,2013.02.06
US 2004146163 A1,2004.07.29
刘青龙;谢军;季乔龙.FC加密卡密钥管理系统设计与实现.电子技术应用.2009,(05),全文.

审查员 王春圆

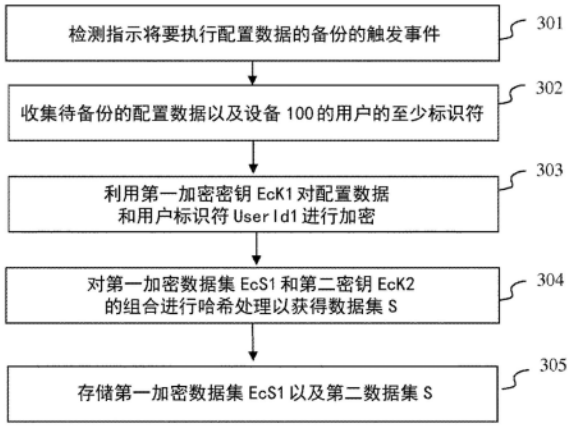
权利要求书1页 说明书7页 附图3页

(54)发明名称

用于执行安全备份和恢复的方法和装置

(57)摘要

提供了用于保存配置数据的备份程序,这些备份程序使得能够在设备被重置为默认设置时在设备上恢复所述配置数据,或者在设备被盗或损坏时在另一设备上恢复所述配置数据。由于配置数据是敏感数据,因此,在整个备份和恢复过程中保护配置数据的机密性和完整性是重要的。目前的解决方案能在同一设备上实现安全的备份和恢复过程,这是因为备份的配置数据采用仅为该设备所知的凭证来进行加密。为了克服这些缺点,提出了一种用于执行安全备份过程的解决方案,该安全备份过程使得能够在相同的设备上或在不同的设备上恢复备份的数据。这通过采用设备池共用的加密密钥来实现。这些共用的加密密钥在设备的制造期间提供。



CN 110431557 B

1.一种用于执行存储在第一设备上的数据的备份以将备份数据恢复到第二设备的方法,所述方法由所述第一设备实现,所述方法包括:

-所述第一设备包括第一预先提供的密钥和第二预先提供的密钥,所述第一预先提供的密钥和所述第二预先提供的密钥是包括所述第一设备和所述第二设备的一组设备所共有的;

-使用所述第一预先提供的密钥,通过对所述数据和所述第一设备的用户的至少一个标识符进行加密来获得第一组数据;

-通过对所述第一组数据和所述第二预先提供的密钥的组合进行哈希处理来获得第二组数据;

-通过存储所述第一组数据和所述第二组数据来备份来自所述第一设备的数据。

2.根据权利要求1所述的方法,其中,所述第一预先提供的密钥是对称加密密钥。

3.根据权利要求1所述的方法,其中,所述第二预先提供的密钥是公共密钥。

4.根据权利要求1所述的方法,其中,按照有规律的时间间隔执行所述备份。

5.根据权利要求1所述的方法,其中,所述备份由在所述第一设备的用户界面上检测到的动作触发。

6.一种用于将备份数据从第一设备恢复到第二设备的方法,所述方法由所述第二设备实现,所述方法包括:

-所述第二设备包括第一预先提供的密钥和第二预先提供的密钥,所述第一预先提供的密钥和所述第二预先提供的密钥是包括所述第一设备和所述第二设备的一组设备所共有的;

-从所述备份数据中检索第一组数据和第二组数据;

-在所述第二设备中,通过对检索到的第一组数据和所述第二预先提供的密钥的组合进行哈希处理来获得第三组数据;

-在获取到的第三组数据与检索到的第二组数据相同的条件下,通过使用所述第一预先提供的密钥对检索到的第一组数据进行解密来获得解密后的第一组数据,并从解密后的第一组数据中检索恢复数据和所述第一设备的用户的至少一个标识符,并且在检索到的所述第一设备的用户的至少一个标识符与提供给所述第二设备的第二用户标识符相同的条件下,将所述恢复数据恢复到所述第二设备。

7.一种第一装置,所述第一装置包括处理器,所述处理器被配置为执行根据权利要求1至5中任一项所述的方法。

8.一种第二装置,所述第二装置包括处理器,所述处理器被配置为执行根据权利要求6所述的方法。

9.一种处理器可读介质,所述处理器可读介质内存储有用于使处理器执行根据权利要求1至5中任一项所述的方法的指令。

10.一种处理器可读介质,所述处理器可读介质内存储有用于使处理器执行根据权利要求6所述的方法的指令。

用于执行安全备份和恢复的方法和装置

技术领域

[0001] 本发明涉及用于恢复配置数据的解决方案。更具体地，本发明涉及用于执行配置数据的安全备份以及使所述备份数据轻松恢复的方法。

背景技术

[0002] 为了根据用户需求来发挥作用，诸如住宅网关、接入点、中继器、移动电话、计算机等现有通信设备根据不同的设置进行配置。

[0003] 提供了用于保存这些配置数据的备份程序，这些备份程序能够在设备被重置为默认设置时在该设备上恢复所述配置数据，或者在设备被盗或损坏时在另一设备上恢复所述配置数据。

[0004] 由于配置数据是敏感数据，因此，在整个备份和恢复过程中保护配置数据的机密性和完整性是非常重要的。

[0005] 目前的解决方案能在同一设备上实现安全的备份和恢复过程，这是因为备份的配置数据采用仅为该设备所知的凭证来进行加密。

[0006] 因此，如果要在另一个设备上恢复配置数据，那么，配置数据应以明文形式进行存储(即，不对配置数据进行加密)，从而允许在所述另一个设备上进行恢复。这种安全性的缺失是现有备份及恢复解决方案的主要缺点所在。

[0007] 在考虑前述内容的基础上，设计出了本发明。

发明内容

[0008] 根据本发明的第一方面，提供了一种用于执行第一设备的配置数据的安全备份的计算机实现的方法，所述方法包括：

[0009] -使用存储在所述第一设备的只读存储器中的第一预先提供的加密密钥，对所述配置数据和所述第一设备的用户的至少一个标识符进行加密，

[0010] -对通过对加密的配置数据和所述第一设备的所述用户的所述至少一个标识符以及存储在所述第一设备的所述只读存储器中的第二预先提供的密钥的组合进行哈希处理而获得的数据集进行加密，

[0011] -存储加密的配置数据和所述第一设备的所述用户的至少一个标识符以及加密数据集。

[0012] 这种解决方案提供了能够在同一设备上或在不同设备上恢复备份数据的安全备份过程。这可以通过使用对设备池共用并且预加载在所述设备的存储器中的加密密钥来实现，其中该设备例如是同一产品型号的设备，或者是由同一公司制造的另一产品型号的设备。

[0013] 例如，这些共用的加密密钥在设备的制造期间提供，并存储在设备的存储器的一部分中。

[0014] 在本发明的实施例中，第一预先提供的加密密钥是对称加密密钥。

[0015] 在本发明的实施例中，第二预先提供的加密密钥是公共密钥。

[0016] 在本发明的实施例中，按照有规律的时间间隔执行安全备份。

[0017] 这样的实施例不需要来自设备的用户的动作。它实现根据配置数据的敏感度进行的被证明有用的定期备份。

[0018] 在本发明的实施例中，安全备份由在第一设备的用户界面上检测到的动作触发。

[0019] 设备的用户可以根据他/她的需求触发配置数据的备份。

[0020] 本发明的另一个目的涉及一种用于恢复第一设备上配置数据的计算机实现的方法，所述方法包括：

[0021] -使用存储在所述第一设备的只读存储器中的第一预先提供的密钥，检查与待恢复的所述配置数据有关的第二数据集的完整性，

[0022] -当检查所述第二数据集的所述完整性时，使用存储在所述第一设备的所述只读存储器中的第二预先提供的解密密钥来对包括所述配置数据在内的第二数据集进行解密，

[0023] -当解密的第二数据集中包括的所述第一设备的用户的至少一个标识符与提供给所述第一设备的所述第一设备的所述用户的至少一个标识符匹配时，恢复所述配置数据。

[0024] 这样的解决方案使得能够在第二设备上恢复在第一设备上安全备份的数据。这可以通过使用对设备池共用的预先提供的解密密钥来实现，其中该设备例如是同一产品型号的设备，或者是由同一公司制造的另一产品型号的设备。

[0025] 例如，这些共用的预先提供的解密密钥在设备的制造期间提供，并存储在设备的存储器的一部分中。因此，可以使用这些解密密钥来对利用加密密钥加密的数据进行解密，其中在备份过程期间，相同的设备使用这些加密密钥来对它们的配置数据进行加密。

[0026] 在这样的解决方案中，由于在没有检查到待恢复数据的完整性的情况下会停止恢复过程，因而确保了备份数据的完整性。

[0027] 此外，为了提高整个过程的安全性，仅在最终检查完成后才在设备上恢复数据。这种最终检查包括：验证执行备份的设备的用户与将要恢复数据的设备的用户相同的用户。这种检查是重要的，因为不同的设备使用相同的加密及解密密钥。

[0028] 在本发明的实施例中，检查第二数据集的完整性包括：

[0029] -通过对第二加密数据集和所述第一预先提供的密钥的组合进行哈希处理来生成第三数据集，

[0030] -将所述第一数据集与所述第三数据集进行比较，

[0031] 当所述第一数据集与所述第三数据集相同时，检查所述第一数据集的所述完整性。

[0032] 本发明的另一个目的是一种能够执行配置数据的安全备份的装置，所述装置包括处理器，所述处理器被配置为：

[0033] -在第一设备的生产期间对所述配置数据和所述第一设备的用户的至少一个标识符进行加密，并将其存储在所述第一设备的只读存储器中，

[0034] -对通过对加密的配置数据和所述第一设备的用户的至少一个标识符以及存储在所述第一设备的所述只读存储器中的第二预先提供的密钥的组合进行哈希处理而获得的数据集进行加密，

[0035] -存储加密的配置数据和所述第一设备的用户的至少一个标识符以及加密数据

集。

[0036] 本发明的另一个目的是一种能够恢复第一设备上的配置数据的装置，所述装置包括处理器，所述处理器被配置为：

[0037] -使用存储在所述第一设备的只读存储器中的第一预先提供的密钥，检查与待恢复的配置数据有关的第二数据集的完整性，

[0038] -当检查第二数据集的完整性时，使用存储在所述第一设备的所述只读存储器中的第二预先提供的解密密钥来对包括所述配置数据在内的第二数据集进行解密，

[0039] -当解密的第二数据集中包括的所述第一设备的用户的至少一个标识符与提供给所述第一设备的所述第一设备的所述用户的至少一个标识符匹配时，恢复所述配置数据。

[0040] 由本发明的元件实现的一些过程可以由计算机实现。因此，这些元件可以采用完全硬件实施例、完全软件实施例(包括固件、常驻软件、微代码等)或者将软件和硬件方面加以组合的实施例的形式，所述软件和硬件方面在本文中通常都可以被称为“电路”、“模块”或“系统”。此外，这些元件可以采用包含在任何有形表达介质中的计算机程序产品的形式，所述有形表达介质具有包含在该介质中的计算机可用程序代码。

[0041] 由于本发明的元件可以用软件实现，因此，本发明可以体现为在任何合适的载体介质上提供给可编程装置的计算机可读代码。有形载体介质可以包括存储介质，比如，软盘、CD-ROM、硬盘驱动器、磁带设备或固态存储设备等。瞬变载体介质可以包括信号，比如，电信号、电子信号、光学信号、声学信号、磁性信号或电磁信号(例如，微波或RF信号)。

附图说明

[0042] 现在将仅通过示例并参考以下附图来描述本发明的实施例，其中：

[0043] 图1表示根据本发明实施例的实现备份和恢复方法的通信设备，

[0044] 图2是示出了根据本发明实施例的通信设备的示例的示意性框图，

[0045] 图3表示根据本发明实施例的对用于执行配置数据的安全备份的过程进行说明的流程图，

[0046] 图4表示根据本发明实施例的对用于恢复安全备份的配置数据的过程进行说明的流程图。

具体实施方式

[0047] 如本领域技术人员将理解的，本原理的各个方面可以体现为系统、方法或计算机可读介质。因此，本原理的各个方面可以采用完全硬件实施例、完全软件实施例(包括固件、常驻软件、微代码等)或者将软件和硬件方面加以组合的实施例的形式，所述软件和硬件方面在本文中通常都可以被称为“电路”、“模块”或“系统”。此外，本原理的各个方面可以采用计算机可读存储介质的形式。可以利用一个或多个计算机可读存储介质的任意组合。

[0048] 如图1所示，第一通信设备100是家庭网关。第一通信设备100包括用于与例如宽带网络进行通信的至少一个网络接口110。例如，这样的网络接口110配置为使用xDSL(x数字订户线)从DSLAM(数字订户线接入复用器)接收数据并向其发送数据，并且还通过光纤从OLT(光线路终端)接收数据并向其发送数据。

[0049] 在本发明的实施例中，第一通信设备100可以嵌入无线传输接口和有线传输接口。

[0050] 图2是示出了根据本发明实施例的第一通信设备100的示例的示意性框图。

[0051] 第一通信设备100包括通过总线206连接的处理器201、存储单元202、输入设备203、显示设备204和接口单元205。当然，可以通过总线连接以外的连接将第一通信设备100的组成元件连接起来。

[0052] 处理器201控制第一通信设备100的操作。存储单元202存储将由处理器201执行的能够执行第一通信设备100的配置数据的安全备份和恢复的至少一个程序、处理器201所执行的计算所使用的各种数据、参数以及处理器201所执行的计算的中间数据等。处理器201可以由任何已知且合适的硬件或软件或硬件和软件的组合形成。例如，处理器201可以由专用硬件(如处理电路)形成，或者由执行存储在其存储器中的程序的可编程处理单元(如CPU(中央处理单元))形成。

[0053] 存储单元202可以由能够以计算机可读方式存储程序、数据等的任何合适的存储设备或装置形成。存储单元202的示例包括诸如半导体存储器器件之类的非暂时性计算机可读存储介质，以及加载到读写单元中的磁性、光学或磁光记录介质。该程序使得处理器201执行根据本公开实施例的安全备份和恢复过程，如下文参考图3和图4所述。

[0054] 输入设备203可以由用户用来输入命令的键盘、指向设备(如鼠标)等形成，以使得用户能选出用于选择要使用的传输接口的参数。输出设备204可以由显示设备形成，以显示例如图形用户界面(GUI)。例如，输入设备203和输出设备204可以通过触摸屏面板一体成型。

[0055] 接口单元205提供第一通信设备100与外部装置之间的接口。接口单元205可以经由线缆或无线通信与外部装置进行通信。在实施例中，外部装置可以是光学采集系统，例如真实相机。

[0056] 本发明可以在除网关之外的设备中执行，例如移动电话、计算机、捕获器等。

[0057] 图3是对用于执行配置数据的安全备份的过程进行说明的流程图。本发明依赖于在将要对数据进行备份的设备与将要恢复所述备份的数据的设备之间使用共享秘密(如加密和密钥)。这两个设备可以是同一个设备或不同的设备。设备的用户无需使用共享秘密来配置该设备。

[0058] 在步骤301中，处理器201检测指示将要执行设备100的配置数据的备份的触发事件(trigger)。

[0059] 在本发明的第一实施例中，触发事件是计时器的到期。例如，根据配置数据的敏感度，按照每天或每小时或每X分钟等频率来安排设备100的配置数据的备份。

[0060] 在本发明的另一实施例中，触发事件是检测到输入设备203上的动作。在这种情况下，检测到此动作会触发备份过程。

[0061] 在步骤302中，处理器201收集待备份的配置数据以及设备100的用户的至少标识符UserId1，如客户标识符、电话号码等。

[0062] 在步骤303中，使用第一预先提供的加密密钥EcK1对配置数据和用户标识符UserId1进行加密。那些加密数据包含第一加密数据集EcS1。

[0063] 例如，这样的第一加密密钥EcK1在设备100的制造期间提供，并且更普遍地在产品型号与设备100相同的所有设备中或同一制造商的其他产品型号的设备中提供。第一预先提供的加密密钥EcK1包含由硬件安全模块(HSM)创建的真正随机数据。第一预先提供的加

密密钥EcK1被存储在存储单元202的分区中。

[0064] 第一预先提供的加密密钥是根据例如AES-256协议(高级加密标准)的对称密钥。

[0065] 第一预先提供的加密密钥EcK1也可以由处理器201使用产品型号与设备100相同的所有设备或同一制造商的其他产品型号的设备共用的加密以及产品型号的标识符和设备100的标识符(如序列号)来生成。

[0066] 在步骤304中,例如,通过使用HMAC方案(密钥哈希消息认证码)对第一预先提供的加密数据集EcS1和第二预先提供的密钥EcK2的组合进行哈希处理来获得第二数据集S。

[0067] 例如,这样的第二预先提供的密钥EcK2在设备100的制造期间提供,并且更普遍地在产品型号与设备100相同的所有设备中或同一制造商的其他产品型号的设备中提供。第二预先提供的密钥EcK2包含由硬件安全模块(HSM)创建的真正随机数据。第二预先提供的密钥EcK2被存储在存储单元202的分区中。

[0068] 第二预先的提供密钥EcK2也可以由处理器201使用产品型号与设备100相同的所有设备或同一制造商的其他产品型号的设备共用的加密以及产品型号的标识符和设备100的标识符(如序列号)来生成。

[0069] 在本发明的实施例中,第一预先提供的加密密钥EcK1和第二预先提供的密钥EcK2由第三方(比如,设备100的制造商或对设备100进行管理的提供商)发送给设备100。第一预先提供的加密密钥EcK1和第二预先提供的密钥EcK2对于产品型号与设备100相同的所有设备或同一制造商的其他产品型号的设备而言是共有的,从而使得能在不同设备之间共享秘密。

[0070] 在步骤304期间获得的第二数据集S用于在恢复过程期间检查备份的配置数据的完整性。

[0071] 在步骤305中,处理器201存储第一加密数据集EcS1以及第二数据集S,其中该第一加密数据集EcS1包括加密的配置数据和设备100的用户的至少一个标识符。

[0072] 这些数据被存储在设备100的存储单元202中,或者存储在远程服务器中。后一实施例使得能够远程获取在设备上对配置进行恢复所需的数据。

[0073] 图4是对用于恢复安全备份的配置数据的过程进行说明的流程图。本发明依赖于在将要对数据进行备份的设备与将要恢复所述备份的数据的设备之间使用共享秘密(如加密和密钥)。这两个设备可以是同一个设备或不同的设备。设备的用户无需使用共享秘密来配置该设备。

[0074] 在步骤401中,处理器201检测指示将要执行设备100的配置数据的恢复的触发事件。

[0075] 在本发明的实施例中,触发事件是检测到输入设备203上的动作,比如,重置命令或启动命令。在另一实施例中,触发事件是检测到输入设备203上的动作。在这种情况下,检测到此动作会触发恢复过程。

[0076] 在步骤402中,处理器201获取第一数据集S和第二加密数据集EcS1。第一数据集S用于检查第二加密数据集EcS1的完整性,而第二加密数据集EcS1包括完成恢复过程所需的配置数据。

[0077] 在实施例中,配置的恢复发生在同一设备100上。在这种情况下,处理器201可以获取存储单元202中的第一数据集S和第二加密数据集EcS1。

[0078] 在另一实施例中,配置的恢复发生在另一个设备上,比如,产品型号与设备100相同的设备或同一制造商的另一产品型号的设备。在这种情况下,处理器201可以从远程服务器获取第一数据集S和第二加密数据集EcS1。

[0079] 在步骤403中,处理器201检查第二加密数据集EcS1的完整性。处理器201使用第一预先提供的密钥DcK2来检查所述第二加密数据集EcS1的完整性,其中该第一预先提供的密钥DcK2与在参考图3描述的备份过程期间使用的第二预先提供的密钥EcK2相对应。

[0080] 例如,第一预先提供的密钥DcK2在设备100的制造期间提供,并且更普遍地在产品型号与设备100相同的所有设备中或同一制造商的其他产品型号的设备中提供。第一预先提供的密钥DcK2包含由硬件安全模块(HSM)创建的真正随机数据。第一预先提供的密钥DcK2被存储在存储单元202的分区中。

[0081] 第一预先提供的密钥DcK2也可以由处理器201使用产品型号与设备100相同的所有设备或同一制造商的其他产品型号的设备共用的加密以及产品型号的标识符和设备100的标识符(如序列号)来生成。

[0082] 处理器201通过使用例如HMAC方案对第二加密数据集EcS1和第二预先提供的密钥EcK2的组合进行哈希处理来生成第三数据集S',并将第一数据集S与第三数据集S'进行比较。

[0083] 如果第一数据集S与第三数据集S'相同,则处理器201执行步骤404,如果第一数据集S与第三数据集S'不同,则停止恢复过程。

[0084] 在步骤404期间,处理器201使用第二预先提供的解密密钥DcK1对第二加密数据集EcS1进行解密,其中该第二预先提供的解密密钥DcK1与在参考图3描述的备份过程期间使用的第一预先提供的加密密钥EcK1相对应。

[0085] 例如,第二预先提供的解密密钥DcK1在设备100的制造期间提供,并且更普遍地在产品型号与设备100相同的所有设备中或同一制造商的其他产品型号的设备中提供。第二预先提供的解密密钥DcK1包含由硬件安全模块(HSM)创建的真正随机数据。第二解密密钥DcK1被存储在存储单元202的分区中。

[0086] 第二预先提供的解密密钥DcK1是根据AES-256协议(高级加密标准)的对称密钥。

[0087] 第二预先提供的解密密钥DcK1也可以由处理器201使用产品型号与设备100相同的所有设备或同一制造商的其他产品型号的设备共用的加密以及产品型号的标识符和设备100的标识符(如序列号)来生成。

[0088] 第一预先提供的密钥DcK2和第二预先提供的解密密钥DcK1对于产品型号与设备100相同的所有设备或同一制造商的其他产品型号的设备而言是共有的,从而使得能在不同设备之间共享秘密。

[0089] 在本发明的实施例中,第一预先提供的密钥DcK2和第二预先提供的解密密钥DcK1由第三方(比如,设备100的制造商或对设备100进行管理的提供商)发送给设备100。

[0090] 如果无法实现第二加密数据集EcS1的解密(这意味着执行恢复过程的设备不是授权设备),则停止恢复过程。

[0091] 如果第二加密数据集EcS1的解密成功,则处理器201获取配置数据以及至少一个用户标识符UserId1。

[0092] 在步骤405中,处理器201将在步骤404期间获取的用户标识符UserId1与在本地提

供给执行恢复过程的设备的第二用户标识符UserId2进行比较。第一用户标识符UserId1和第二用户标识符UserId2可以是相同的，例如，它们可以是设备100的用户的电话号码。

[0093] 如果这两个用户标识符UserId1和UserId2匹配，则处理器201可以执行配置数据的恢复，如果用户标识符UserId1和UserId2不匹配，则停止恢复过程。

[0094] 第二用户标识符UserId2可以通过输入设备203在本地提供，或者在恢复过程开始之前使用诸如TR-69之类的过程来远程提供。

[0095] 尽管上文已经参考特定实施例描述了本发明，但是，本发明并不局限于特定实施例，并且对于本领域技术人员来说，在本发明范围内的修改是显而易见的。

[0096] 本领域技术人员在参考前述说明性实施例时将认识到许多进一步的修改和变型，这些说明性实施例仅作为示例给出，并不旨在限制仅由所附权利要求确定的本发明的范围。特别地，在适当的情况下，来自不同实施例的不同特征可以进行互换。

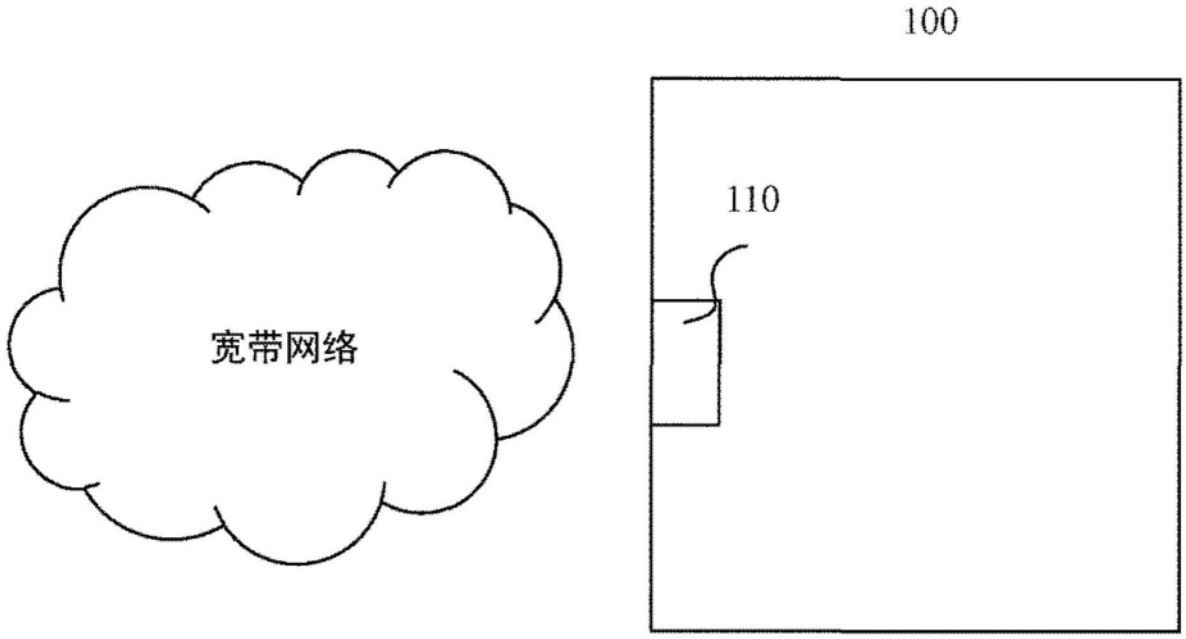

100
110
宽带网络

图1

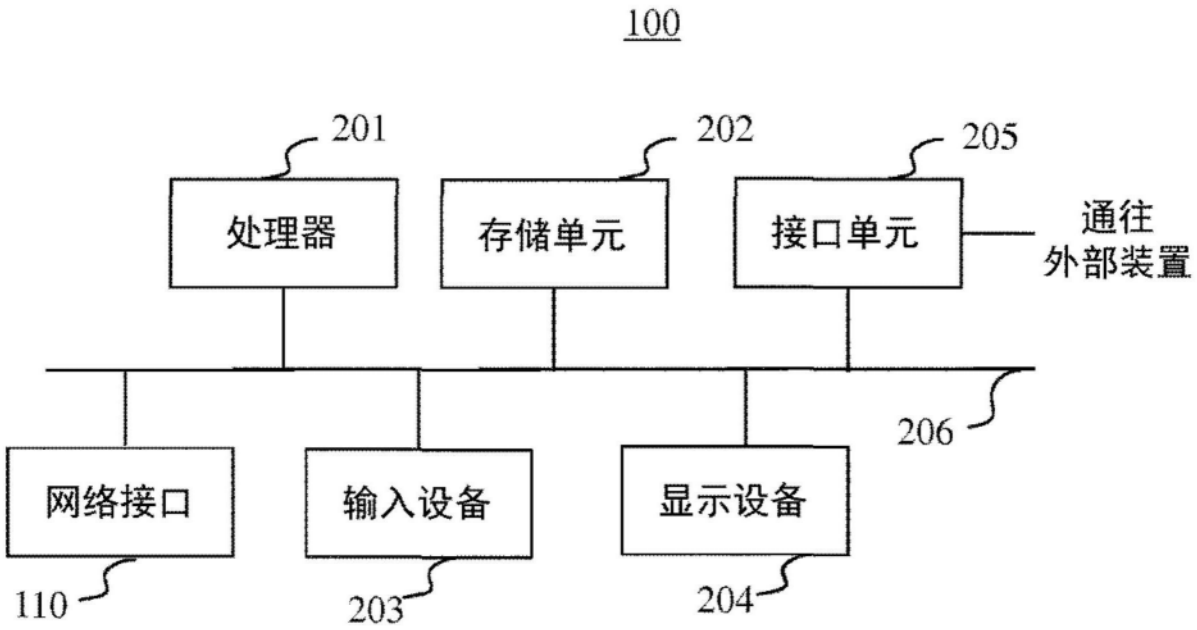

100
201
202
205
处理器
存储单元
接口单元
通往
外部装置
206
网络接口
输入设备
显示设备
110
203
204

图2

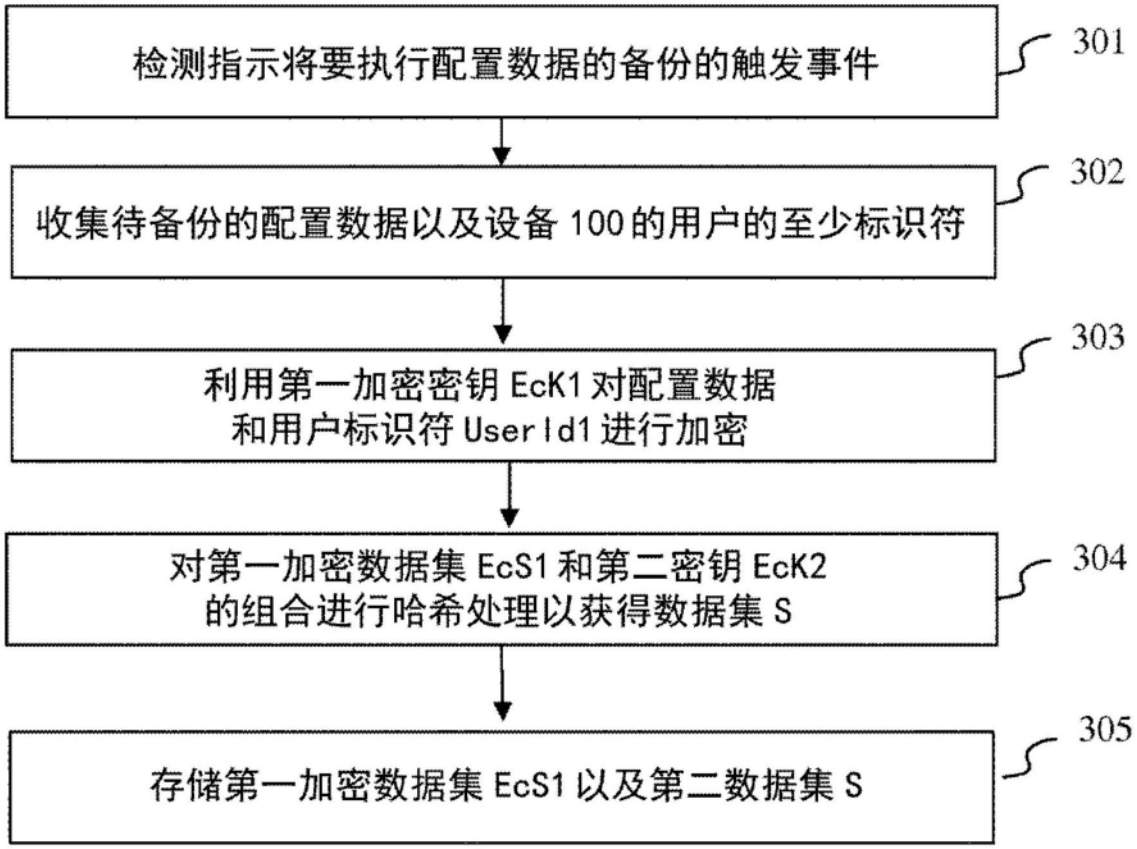

检测指示将要执行配置数据的备份的触发事件
301
收集待备份的配置数据以及设备 100 的用户的至少标识符
302
利用第一加密密钥 EcK1 对配置数据
和用户标识符 UserId1 进行加密
303
对第一加密数据集 EcS1 和第二密钥 EcK2
的组合进行哈希处理以获得数据集 S
304
存储第一加密数据集 EcS1 以及第二数据集 S
305

图3

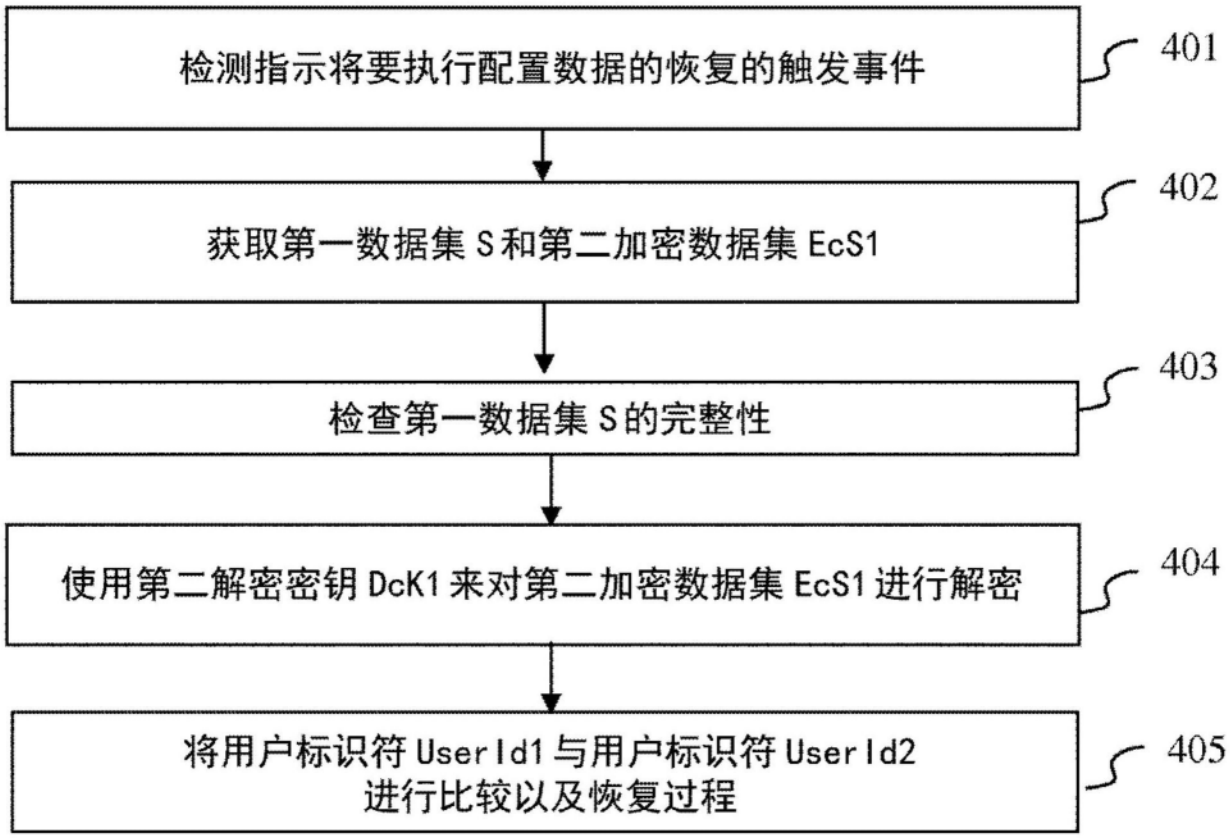

检测指示将要执行配置数据的恢复的触发事件
401
获取第一数据集 S 和第二加密数据集 EcS1
402
检查第一数据集 S 的完整性
403
使用第二解密密钥 DcK1 来对第二加密数据集 EcS1 进行解密
404
将用户标识符 UserId1 与用户标识符 UserId2
进行比较以及恢复过程
405

图4