(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 106683242 A
(43)申请公布日 2017.05.17

(21)申请号 201611111468.3

(22)申请日 2016.12.02

(71)申请人 歌尔科技有限公司
地址 266104 山东省青岛市崂山区北宅街道投资服务中心308室

(72)发明人 姜茂山 陈翔 孔坚

(74)专利代理机构 北京市隆安律师事务所 11323
代理人 权鲜枝 吴昊

(51)Int.Cl.
G07C 9/00(2006.01)
E05B 45/06(2006.01)

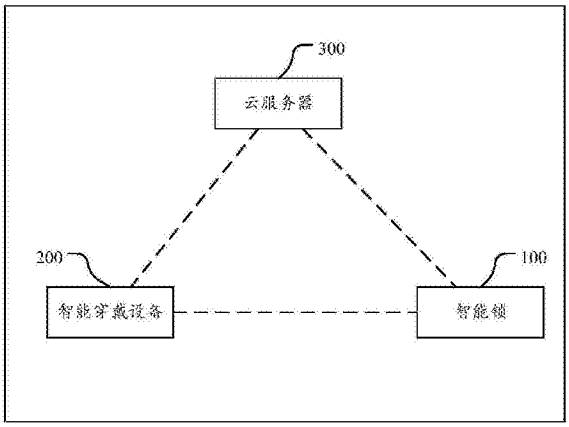
权利要求书2页 说明书5页 附图3页

(54)发明名称

一种智能锁系统、智能锁及智能穿戴设备

(57)摘要

本发明公开了一种智能锁系统、智能锁及智能穿戴设备，智能锁系统包括：智能锁、智能穿戴设备和云服务器；智能穿戴设备接收用户输入的智能锁的ID号码和对应的开锁密码，并将接收的用户输入的开锁密码保存至自身，并将自身物理地址、智能锁的ID号码和开锁密码上传至云服务器保存。云服务器将接收的智能穿戴设备的物理地址和开锁密码推送至对应ID号码的智能锁中进行保存。智能锁用于当与智能穿戴设备建立近场通信连接时，读取智能穿戴设备的物理地址和其内的开锁密码，并与自身保存的该物理地址对应的开锁密码比对，在一致时开锁。用户无需额外随身携带钥匙，开锁更加方便快捷。



CN 106683242 A

1.一种智能锁系统，其特征在于，包括：智能锁、智能穿戴设备和云服务器；

所述智能穿戴设备，用于接收用户输入的智能锁的ID号码和对应的开锁密码，并与所述云服务器建立移动通信连接，将接收的用户输入的开锁密码保存至自身，并将自身物理地址、所述智能锁的ID号码和所述开锁密码上传至所述云服务器保存；

所述云服务器，与所述智能锁建立无线通信连接，用于获取所述智能锁在首次被激活时上传的ID号码；以及将接收的所述智能穿戴设备的物理地址和所述开锁密码推送至对应ID号码的智能锁中进行保存；

所述智能锁，用于当与所述智能穿戴设备建立近场通信连接时，读取所述智能穿戴设备的物理地址和其内的开锁密码，并与自身保存的该物理地址对应的开锁密码比对，在一致时开锁。

2.根据权利要求1所述的智能锁系统，其特征在于，

所述智能穿戴设备，还用于在接收用户输入的智能锁的ID号码和开锁密码之前，开启权限设置界面，接收用户在所述权限设置界面输入的权限账号和权限密码，并上传至所述云服务器保存，在所述智能穿戴设备重置所述智能锁的开锁密码时需要重新输入所述权限账号和所述权限密码进行验证。

3.根据权利要求1所述的智能锁系统，其特征在于，所述智能穿戴设备，还用于对接收的用户输入并保存至自身的开锁密码进行AES加密；

所述智能锁，还用于对从所述智能穿戴设备内读取的开锁密码进行AES解密，将解密后的开锁密码与自身保存的所述智能穿戴设备的物理地址对应的开锁密码比对。

4.根据权利要求2所述的智能锁系统，其特征在于，所述智能锁系统还包括：智能移动终端，

所述智能移动终端，与所述智能穿戴设备建立无线通信连接，用于为所述智能穿戴设备提供输入界面，接收用户输入的权限账号、权限密码以及所述智能锁的ID号码和对应的开锁密码发送至所述智能穿戴设备。

5.根据权利要求1所述的智能锁系统，其特征在于，所述智能锁上包括密码管理按键，所述密码管理按键被按下时，所述智能锁删除自身保存的智能穿戴设备的物理地址及其对应的开锁密码，并与所述云服务器建立无线通信连接，通知所述云服务器删除所保存的与自身的ID号码相关的数据。

6.一种智能锁，其特征在于，包括存储器、微处理器、NFC模块和WIFI模块；

所述存储器，用于存储智能穿戴设备物理地址及其对应的开锁密码；

所述NFC模块，用于与所述智能穿戴设备建立近场通信连接；

所述WIFI模块，用于与云服务器建立无线通信连接，所述云服务器中保存有所述智能穿戴设备上传的物理地址、所述智能锁的ID号码和所述开锁密码；

所述微处理器，用于在首次被激活时上传自身的ID号码给所述云服务器，接收所述云服务器根据所述ID号码推送的所述智能穿戴设备的物理地址及其对应的开锁密码；当与所述智能穿戴设备建立近场通信连接时，读取所述智能穿戴设备的物理地址和其内的开锁密码，并与自身保存的该物理地址对应的开锁密码比对，在一致时开锁。

7.根据权利要求6所述的智能锁，其特征在于，还包括解密模块，用于对从所述智能穿戴设备内读取的开锁密码进行AES解密，将解密后的开锁密码与自身保存的所述智能穿戴

设备的物理地址对应的开锁密码比对。

8.根据权利要求6所述的智能锁，其特征在于，还包括密码管理按键，所述密码管理按键被按下时，所述智能锁删除自身保存的智能穿戴设备的物理地址及其对应的开锁密码，并与所述云服务器建立无线通信连接，通知所述云服务器删除所保存的与自身的ID号码相关的数据。

9.一种智能穿戴设备，其特征在于，包括NFC模块、SIM模块、微处理器；

所述NFC模块，用于与智能锁建立近场通信连接；

所述SIM模块，用于与云服务器建立移动通信连接；

所述微处理器，用于将接收的用户输入的开锁密码保存至自身，并将自身物理地址、以及智能锁的ID号码和开锁密码上传至云服务器保存。

10.根据权利要求9所述的智能穿戴设备，其特征在于，所述智能穿戴设备还包括：WIFI模块和/或蓝牙模块；

所述智能穿戴设备通过所述WIFI模块和/或蓝牙模块与外部智能移动终端建立无线通信连接，所述智能移动终端为所述智能穿戴设备提供输入界面，接收用户输入的权限账号、权限密码以及所述智能锁的ID号码和对应的开锁密码发送至所述智能穿戴设备。

一种智能锁系统、智能锁及智能穿戴设备

技术领域

[0001] 本发明涉及智能锁技术领域，特别涉及一种智能锁系统、智能锁及智能穿戴设备。

背景技术

[0002] 目前智能穿戴设备，如智能手表等，越来越普及，但是当前主要被用于计步、睡眠、来电提醒、支付等功能，并没有和我们周围手机之外的电子设备进行交互。

[0003] 目前智能锁的普及也越来越广，大部分还是以使用密码开锁、指纹开锁等技术作为卖点。但是这些智能锁也存在一定的安全隐患，对于密码开锁，密码有被盗取的潜在风险；对于指纹开锁，如果被有心的不法分子使用胶带等工具获取用户的指纹，也可能导致家里被盗。

发明内容

[0004] 鉴于上述问题，本发明提供了一种智能锁系统、智能锁及智能穿戴设备，以解决现有智能锁存在一定的安全隐患的问题。

[0005] 为达到上述目的，本发明的技术方案是这样实现的：

[0006] 一方面，本发明提供一种智能锁系统，包括：智能锁、智能穿戴设备和云服务器；

[0007] 所述智能穿戴设备，用于接收用户输入的智能锁的ID号码和对应的开锁密码，并与所述云服务器建立移动通信连接，将接收的用户输入的开锁密码保存至自身，并将自身物理地址、所述智能锁的ID号码和所述开锁密码上传至所述云服务器保存；

[0008] 所述云服务器，与所述智能锁建立无线通信连接，用于获取所述智能锁在首次被激活时上传的ID号码；以及将接收的所述智能穿戴设备的物理地址和所述开锁密码推送至对应ID号码的智能锁中进行保存；

[0009] 所述智能锁，用于当与所述智能穿戴设备建立近场通信连接时，读取所述智能穿戴设备的物理地址和其内的开锁密码，并与自身保存的该物理地址对应的开锁密码比对，在一致时开锁。

[0010] 另一方面，本发明还提供一种智能锁，包括存储器、微处理器、NFC模块和WIFI模块；

[0011] 所述存储器，用于存储智能穿戴设备物理地址及其对应的开锁密码；

[0012] 所述NFC模块，用于与所述智能穿戴设备建立近场通信连接；

[0013] 所述WIFI模块，用于与云服务器建立无线通信连接，所述云服务器中保存有所述智能穿戴设备上传的物理地址、所述智能锁的ID号码和所述开锁密码；

[0014] 所述微处理器，用于在首次被激活时上传自身的ID号码给所述云服务器，接收所述云服务器根据所述ID号码推送的所述智能穿戴设备的物理地址及其对应的开锁密码；当与所述智能穿戴设备建立近场通信连接时，读取所述智能穿戴设备的物理地址和其内的开锁密码，并与自身保存的该物理地址对应的开锁密码比对，在一致时开锁。

[0015] 另一方面，本发明还提供一种智能穿戴设备，包括NFC模块、SIM模块、微处理器；

[0016] 所述NFC模块，用于与智能锁建立近场通信连接；

[0017] 所述SIM模块，用于与云服务器建立移动通信连接；

[0018] 所述微处理器，用于将接收的用户输入的开锁密码保存至自身，并将自身物理地址、以及智能锁的ID号码和开锁密码上传至云服务器保存。

[0019] 本发明的有益效果是：本发明提供一种智能锁系统、智能锁及智能穿戴设备，智能穿戴设备接收的用户输入的开锁密码保存至自身，并将自身物理地址、智能锁的ID号码和开锁密码上传至云服务器保存。智能穿戴设备将开锁密码上传至云服务器保存，可以在用户忘记开锁密码时从云服务器找回密码。智能锁，用于当与智能穿戴设备建立近场通信连接时，读取智能穿戴设备的物理地址和其内的开锁密码，并与自身保存的该物理地址对应的开锁密码比对，在一致时开锁。智能穿戴设备的物理地址和开锁密码作为开锁的双重保险，只有在二者均与智能锁中保存的信息一致时才能开锁，增强了智能锁系统的安全性能。并且用户不再需要额外随身携带钥匙，开锁更加方便快捷。

附图说明

[0020] 图1是本发明实施例的智能锁系统的一种示意图；

[0021] 图2是本发明实施例的智能锁系统的另一种示意图；

[0022] 图3是本发明实施例的智能锁的一种示意图；

[0023] 图4是本发明实施例的智能锁的另一种示意图；

[0024] 图5是本发明实施例的智能穿戴设备的一种示意图；

[0025] 图6是本发明实施例的智能穿戴设备的另一种示意图。

具体实施方式

[0026] 本发明的设计构思是，利用智能穿戴设备与智能锁建立近场通信连接来开锁。用户预先将智能穿戴设备与智能锁绑定，在智能穿戴设备设置开锁密码并保存至智能穿戴设备，智能穿戴设备将开锁密码和自身物理地址上传至云服务器保存，并将自身物理地址和开锁密码推送至智能锁保存。在后续需要开锁时，将智能穿戴设备靠近智能锁，智能锁检测到智能穿戴设备后自动读取智能穿戴设备的物理地址和其内的开锁密码，当与自身保存的物理地址及其对应的开锁密码比对一致时开锁。因此用户不再需要额外随身携带钥匙，开锁更加方便快捷。

[0027] 为使本发明的目的、技术方案和优点更加清楚，下面将结合附图对本发明实施方式作进一步地详细描述。

[0028] 本发明实施例提供一种智能锁系统，如图1所示，该智能锁系统包括：智能锁100、智能穿戴设备200和云服务器300；

[0029] 智能穿戴设备200，用于接收用户输入的智能锁100的ID号码和对应的开锁密码，并与云服务器300建立移动通信连接，将接收的用户输入的开锁密码保存至自身，并将自身物理地址、智能锁100的ID号码和开锁密码上传至云服务器300保存；云服务器300，与智能锁100建立无线通信连接，用于获取智能锁100在首次被激活时上传的ID号码；以及将接收的智能穿戴设备200的物理地址和开锁密码推送至对应ID号码的智能锁100中进行保存；

[0030] 智能锁100，用于当与智能穿戴设备200建立近场通信连接时，读取智能穿戴设备

200的物理地址和其内的开锁密码，并与自身保存的该物理地址对应的开锁密码比对，在一致时开锁，在不一致时，提示短暂的警报声。

[0031] 由上述可知，在本发明实施例中，智能穿戴设备200的物理地址和开锁密码作为开锁的双重保险，只有在二者均与智能锁100中保存的信息一致时才能开锁，增强了智能锁系统的安全性能。

[0032] 在本发明实施例中，智能穿戴设备200，还用于在接收用户输入的智能锁100的ID号码和开锁密码之前，开启权限设置界面，接收用户在权限设置界面输入的权限账号和权限密码，并上传至云服务器300保存，在智能穿戴设备200重置智能锁100的开锁密码时需要重新输入权限账号和权限密码进行验证。

[0033] 在本发明的一个具体实施例中，智能穿戴设备200上安装有开锁APP，用户打开APP开启权限设置界面，在权限设置界面输入权限账号和权限密码，APP将权限账号和权限密码上传至云服务器300保存。在用户重置智能锁100的开锁密码时需要重新输入权限账号和权限密码进行验证。当智能穿戴设备200丢失时，首先开锁APP必须需要权限账号和权限密码进行登录，且默认不会记住密码，此防范手段可防止不法分子重置开锁密码后进行开锁。

[0034] 权限账号和权限密码设置完成后，用户开启绑定智能锁界面，在APP界面输入待绑定的智能锁100的ID号码，完成该智能穿戴设备200与该ID号码对应的智能锁100的绑定。绑定完成后，输入与该智能锁100对应的开锁密码，智能穿戴设备200将开锁密码保存到本地，完成开锁密码的设置，并与云服务器300建立移动通信连接，将自身物理地址、绑定的智能锁100的ID号码和设置的开锁密码上传至云服务器300保存。

[0035] 由上述可知，在本发明的实施例中，开锁密码除了保存在智能穿戴设备200本地，还上传至云服务器300保存，这样可以方便用户在忘记开锁密码时从云服务器300找回密码。

[0036] 在本发明的一个实施例中，智能穿戴设备200，还用于对接收的用户输入并保存至自身的开锁密码进行AES加密；智能锁100，还用于对从智能穿戴设备200内读取的开锁密码进行AES解密，将解密后的开锁密码与自身保存的智能穿戴设备200的物理地址对应的开锁密码比对。AES加密，即高级加密标准(Advanced Encryption Standard，AES)，是对称密钥加密中最流行的算法之一，当然也可使用其他非对称密钥加密算法。AES加密较难破解，降低了密码被空中拦截后被破解的风险，增强了产品的保密性。

[0037] 在本发明的一个实施例中，为了进一步增强智能锁系统的保密性，对于同一智能锁100，云服务器300按智能锁100的ID号码仅能保存预定个数的智能穿戴设备200的物理地址和开锁密码。例如预定个数为6个，当服务器接收的同一智能锁100绑定的智能穿戴设备200的物理地址和开锁密码超出6个时，云服务器300向最后发送的智能穿戴设备200发送不能保存的提示信息，防止不法分子试图用新的智能穿戴设备200与智能锁100绑定以达到开锁的目的。

[0038] 在本发明的一个实施例中，如图2所示，智能锁系统还包括：智能移动终端400。该智能移动终端400与智能穿戴设备200建立无线通信连接，用于为智能穿戴设备200提供输入界面，接收用户输入的权限账号、权限密码以及智能锁100的ID号码和对应的开锁密码发送至智能穿戴设备200。此时智能移动终端400仅充当智能穿戴设备200的键盘。由于智能穿戴设备200的屏幕不适合设计的很大，目前市面上的智能穿戴设备200屏幕尺寸也都很小，

因此不方便用户在屏幕上直接输入字符。本发明实施例通过无线连接外部智能移动终端400，通过智能移动终端400为智能穿戴设备200提供输入字符界面的方案，很好地解决了该问题。

[0039] 在本发明的一个实施例中，智能穿戴设备200可以为智能手表，如谷歌android wear系统或者是安卓系统的智能手表。智能穿戴设备200与智能锁100均支持近场通信(Near Field Communication，NFC)技术，二者通过NFC建立无线连接。由于NFC的可用通信距离较短，一般为10厘米左右，因此NFC用于智能开锁系统的通信相较于WIFI或者蓝牙更安全。在本发明实施例中，智能锁100被定义为主动式NFC读写器，智能穿戴设备200被定义为被动式标签。

[0040] 智能穿戴设备200与服务器通过移动通信建立连接，可通过在智能穿戴设备200上安装SIM卡实现。智能穿戴设备200与智能移动终端400的无线通信连接可通过设置WIFI模块和/或蓝牙模块实现。智能锁100与服务器的无线通信连接可通过WIFI模块实现。在本发明的实施例中，当智能穿戴设备200丢失时，可通过智能锁100上设置的密码管理按键，删除自身保存的智能穿戴设备200的物理地址及其对应的开锁密码，恢复出厂设置，并将智能锁100与云服务器300建立无线通信连接，通知云服务器300删除所保存的与自身的ID号码相关的数据。例如删除自身存储的智能穿戴设备200的物理地址和开锁密码，同时删除服务器存储的与自身绑定的智能穿戴设备200的物理地址、开锁密码、权限账号和权限密码，防止不法分子盗取智能穿戴设备200后开锁。

[0041] 在本发明实施例中，也可通过智能移动终端400管理智能锁100的密码，在智能移动终端400输入智能锁100的ID号码进入对应的智能锁100的密码管理界面，删除自身保存的智能穿戴设备200的物理地址及其对应的开锁密码。

[0042] 本发明实施例还提供一种智能锁，如图3所示，该智能锁包括存储器140、微处理器110、NFC模块130和WIFI模块120；

[0043] 存储器140，用于存储智能穿戴设备物理地址及其对应的开锁密码；

[0044] NFC模块130，用于与智能穿戴设备建立NFC连接；

[0045] WIFI模块120，用于与云服务器建立无线通信连接，云服务器中保存有智能穿戴设备上传的物理地址、智能锁的ID号码和开锁密码；

[0046] 微处理器110，用于在首次被激活时上传自身的ID号码至云服务器，接收云服务器根据ID号码推送的智能穿戴设备的物理地址及其对应的开锁密码；当与智能穿戴设备建立NFC连接时，读取智能穿戴设备的物理地址和其内的开锁密码，并与自身保存的该物理地址对应的开锁密码比对，在一致时开锁。

[0047] 在本发明实施例中，智能锁还包括报警模块。当智能锁读取智能穿戴设备的物理地址和其内的开锁密码，并与自身保存的该物理地址对应的开锁密码比对，物理地址和开锁密码任一个比对不一致时，报警模块提示短暂的警报声。

[0048] 在本发明的一个实施例中，如图4所示，该智能锁还包括解密模块150，用于对从智能穿戴设备内读取的开锁密码进行AES解密，将解密后的开锁密码与自身保存的智能穿戴设备的物理地址对应的开锁密码比对，增强产品的保密性。

[0049] 在本发明实施例中，如图4所示，该智能锁还包括密码管理按键160，密码管理按键160被按下时，智能锁删除自身保存的智能穿戴设备的物理地址及其对应的开锁密码，并与

云服务器建立无线通信连接，通知云服务器删除所保存的与自身的ID号码相关的数据。

[0050] 本发明实施例还提供一种智能穿戴设备，如图5所示，该智能穿戴设备包括NFC模块220、SIM模块230和微处理器210；

[0051] NFC模块220，用于与智能锁建立近场通信连接；

[0052] SIM模块230，用于与云服务器建立移动通信连接；

[0053] 微处理器210，用于将接收的用户输入的开锁密码保存至自身，并将自身物理地址、以及智能锁的ID号码和开锁密码上传至云服务器保存；以及，在接收到智能锁的。

[0054] 在本发明实施例中，如图6所示，该智能穿戴设备还包括：WIFI模块/蓝牙模块240，当然也可同时设置WIFI模块和蓝牙模块。

[0055] 智能穿戴设备通过WIFI模块/蓝牙模块240与外部智能移动终端建立无线通信连接，智能移动终端为智能穿戴设备提供输入界面，接收用户输入的权限账号、权限密码以及智能锁的ID号码和对应的开锁密码发送至智能穿戴设备。

[0056] 综上所述，本发明实施例提供一种智能锁系统、智能锁及智能穿戴设备，智能穿戴设备接收的用户输入的开锁密码保存至自身，并将自身物理地址、智能锁的ID号码和开锁密码上传至云服务器保存。智能穿戴设备将开锁密码上传至云服务器保存，可以在用户忘记开锁密码时从云服务器找回密码。智能锁，用于当与智能穿戴设备建立近场通信连接时，读取智能穿戴设备的物理地址和其内的开锁密码，并与自身保存的该物理地址对应的开锁密码比对，在一致时开锁。智能穿戴设备的物理地址和开锁密码作为开锁的双重保险，只有在二者均与智能锁中保存的信息一致时才能开锁，增强了智能锁系统的安全性能。并且用户不再需要额外随身携带钥匙，开锁更加方便快捷。

[0057] 以上所述，仅为本发明的具体实施方式，在本发明的上述教导下，本领域技术人员可以在上述实施例的基础上进行其他的改进或变形。本领域技术人员应该明白，上述的具体描述只是更好的解释本发明的目的，本发明的保护范围应以权利要求的保护范围为准。

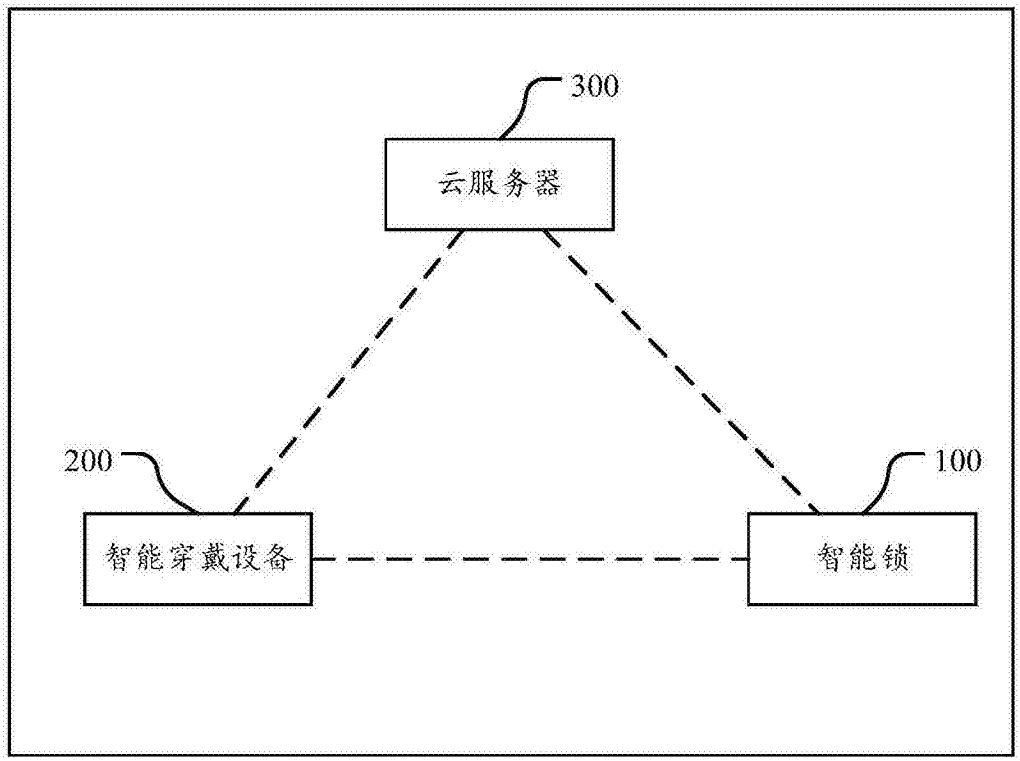

300
云服务器
200
100
智能穿戴设备
智能锁

图1

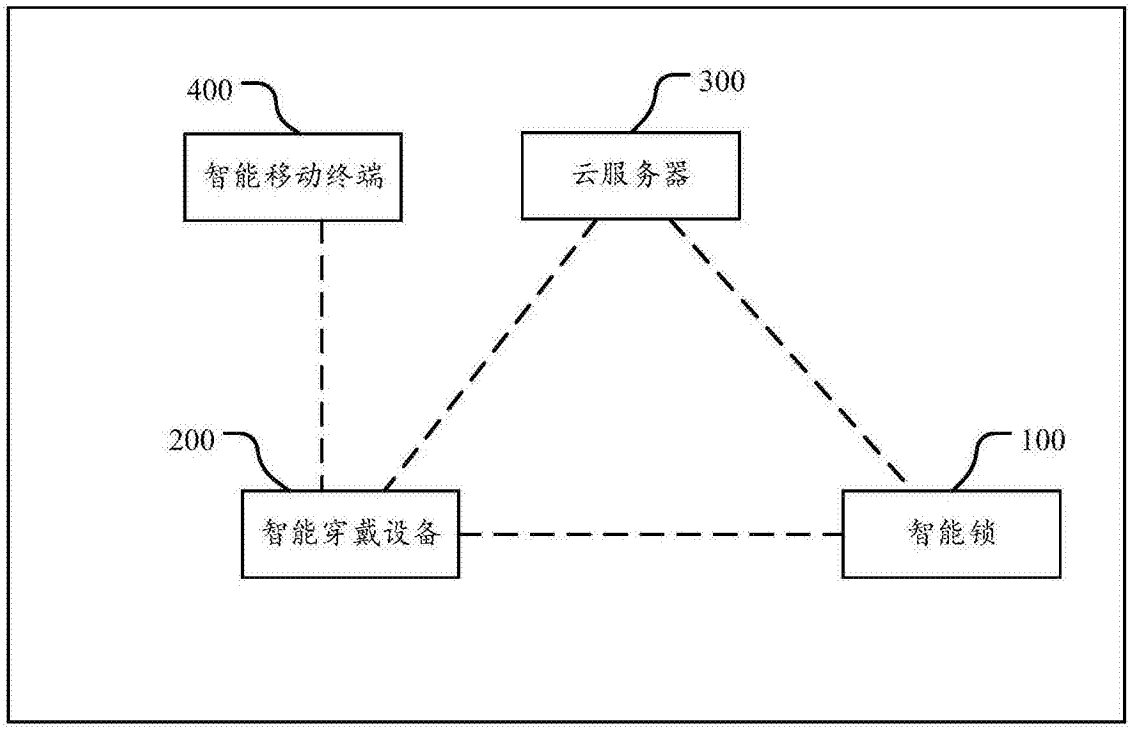

400
智能移动终端
300
云服务器
200
100
智能穿戴设备
智能锁

图2

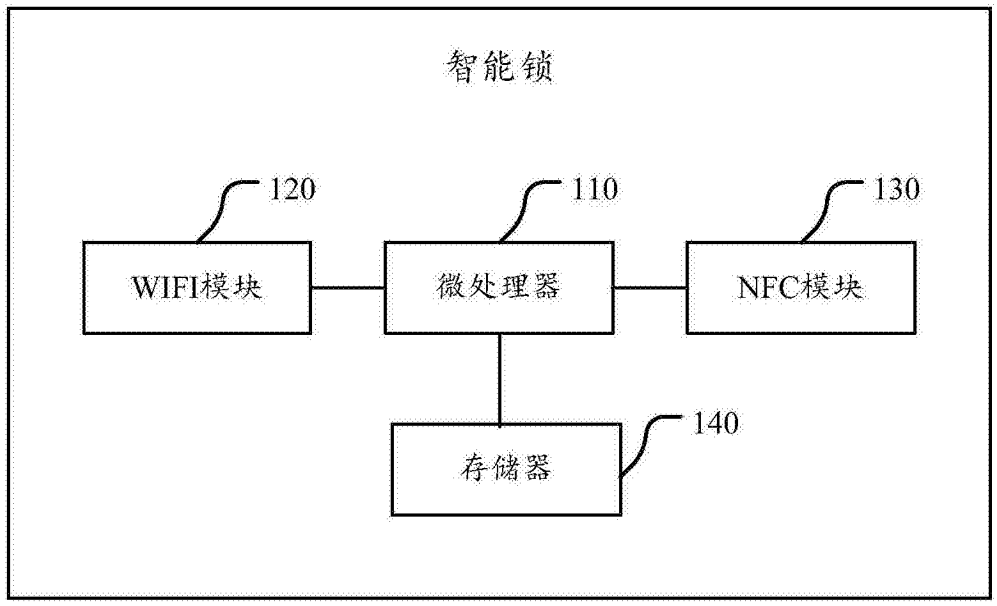

智能锁
120
110
130
WIFI模块
微处理器
NFC模块
140
存储器

图3

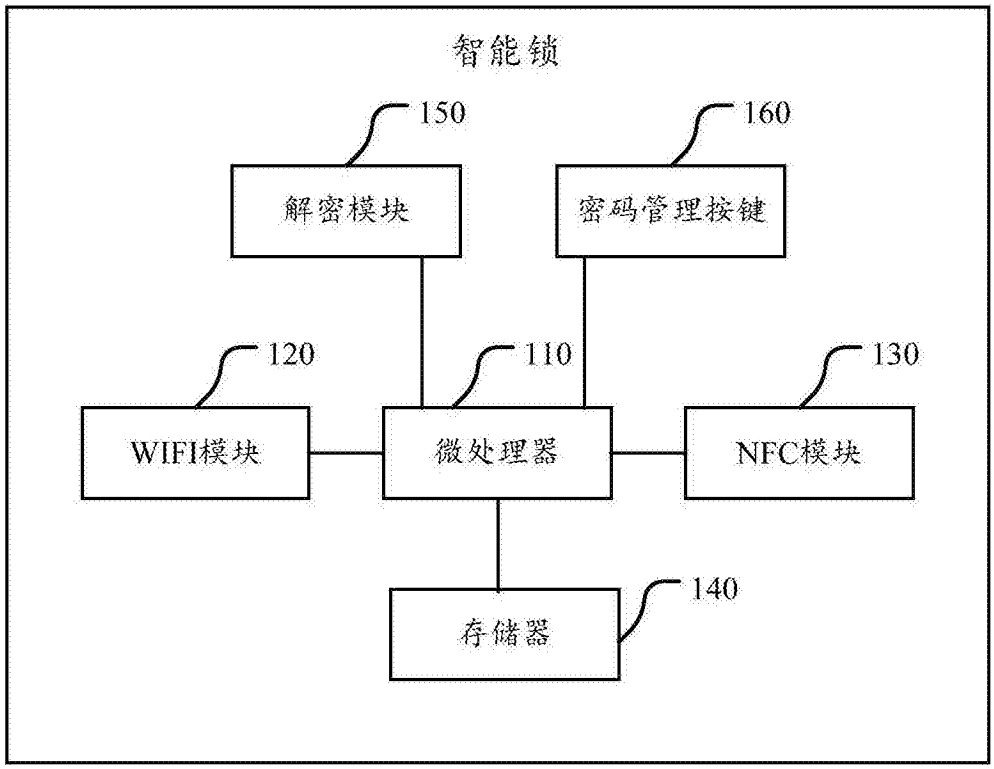

智能锁
150
160
解密模块
密码管理按键
120
110
130
WIFI模块
微处理器
NFC模块
140
存储器

图4

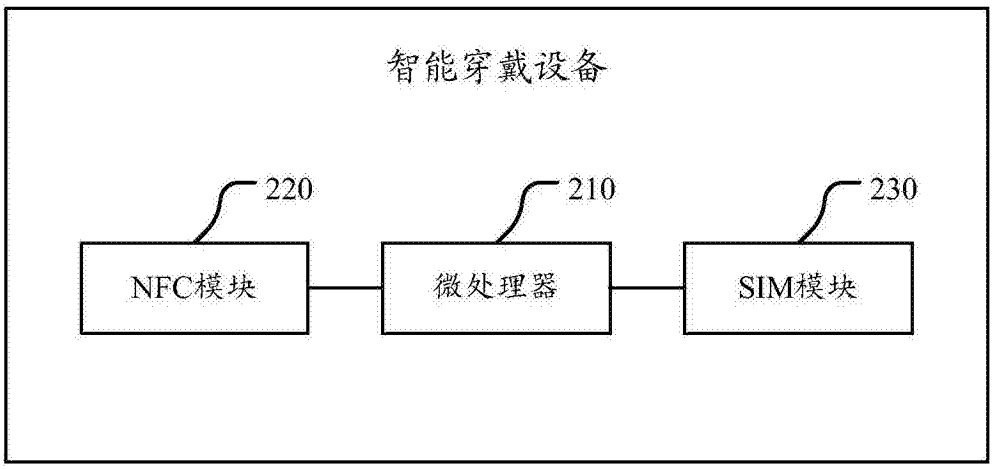

智能穿戴设备
220
210
230
NFC模块
微处理器
SIM模块

图5

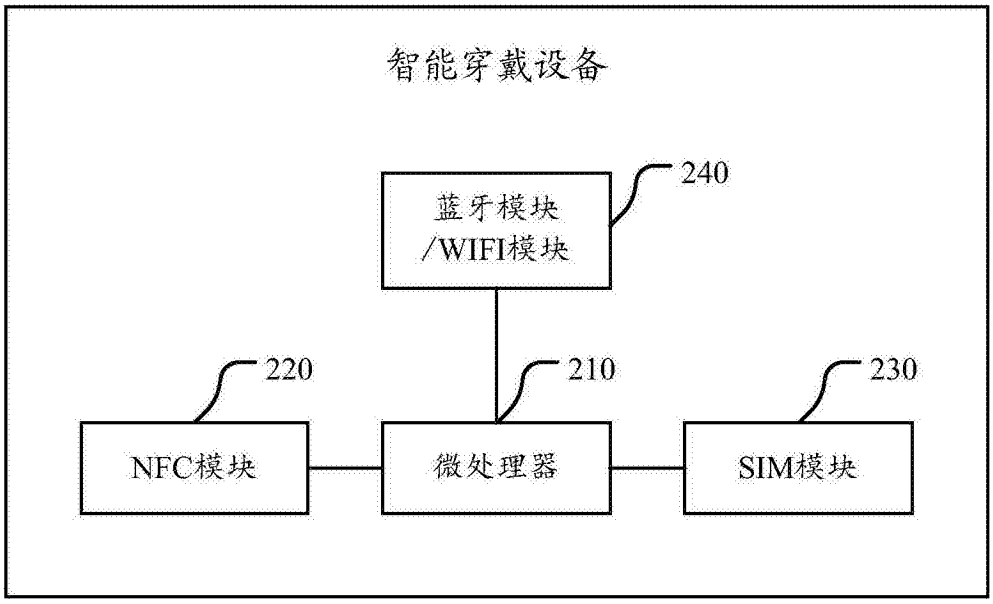

智能穿戴设备
240
蓝牙模块
/WIFI模块
220
210
230
NFC模块
微处理器
SIM模块

图6