[19] Patents Registry
The Hong Kong Special Administrative Region
香港特別行政區
專利註冊處

[11] 1248024 B
CN 107889536 B

[12] **STANDARD PATENT (R) SPECIFICATION**
轉錄標準專利說明書

[21] Application no. 申請編號
18107385.8

[22] Date of filing 提交日期
06.06.2018

[51] Int. Cl.
G07C 9/00 (2020.01) G07C 9/23 (2020.01)
G07C 9/25 (2020.01) E05B 49/00 (2006.01)
H04W 4/80 (2018.01) E05B 47/06 (2006.01)

[54] LOCK AND METHODS FOR REDUNDANT ACCESS CONTROL
用於冗餘接入控制的鎖和方法

[30] Priority 優先權
06.07.2015 US 62/189,193
05.05.2016 US 15/147,759

[43] Date of publication of application 申請發表日期
05.10.2018

[45] Date of publication of grant of patent 批予專利的發表日期
19.03.2021

[86] International application no. 國際申請編號
PCT/IB2016/000968

[87] International publication no. and date 國際申請發表編號及日期
WO2017/006172 12.01.2017

CN Application no. & date 中國專利申請編號及日期
CN 201680028620.3 06.07.2016

CN Publication no. & date 中國專利申請發表編號及日期
CN 107889536 06.04.2018

Date of grant in designated patent office 指定專利當局批予專利日期
10.07.2020

[73] Proprietor 專利所有人
ACSYS IP HOLDING INC.
阿克賽思 IP 控股公司
Verdun 732
P.O. Box 13-5398, Rachid Karamech St. Beirut
LEBANON

[72] Inventor 發明人
BELHADIA, Karim K·貝爾哈迪亞
MOURADIAN, Jean J·穆拉迪安
MEGANCK, David D·麥甘克
FARES, Ahmad A·法雷斯

[74] Agent and / or address for service 代理人及/或送達地址
SPRUSON & FERGUSON (HONG KONG) LIMITED
5001 Hopewell Centre
183 Queen's Road East, Wan Chai
HONG KONG

(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 107889536 B
(45)授权公告日 2020.07.10

(21)申请号 201680028620.3

(22)申请日 2016.07.06

(65)同一申请的已公布的文献号
申请公布号 CN 107889536 A

(43)申请公布日 2018.04.06

(30)优先权数据
62/189,193 2015.07.06 US
15/147,759 2016.05.05 US

(85)PCT国际申请进入国家阶段日
2017.11.17

(86)PCT国际申请的申请数据
PCT/IB2016/000968 2016.07.06

(87)PCT国际申请的公布数据
WO2017/006172 EN 2017.01.12

(73)专利权人 阿克赛思IP控股公司
地址 黎巴嫩贝鲁特

(72)发明人 K·贝尔哈迪亚 J·穆拉迪安
D·麦甘克 A·法雷斯

(74)专利代理机构 北京派特恩知识产权代理有限公司 11270
代理人 康艳青 姚开丽

(51)Int.Cl.
G07C 9/00(2020.01)
G07C 9/23(2020.01)
G07C 9/25(2020.01)
E05B 49/00(2006.01)
H04W 4/80(2018.01)
E05B 47/06(2006.01)

审查员 朱晓琳

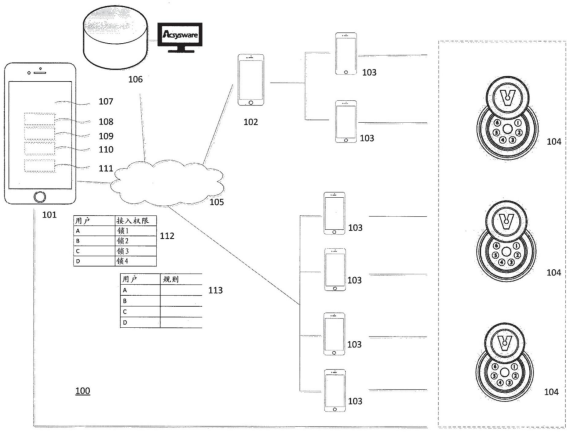
权利要求书3页 说明书18页 附图18页

(54)发明名称

用于冗余接入控制的锁和方法

(57)摘要

公开了用于提供具有可移除无线按钮的冗余接入控制系统的系统和方法。根据本发明的一些实施例，该系统和方法包括具有按钮的智能锁，该按钮能够与网络设备、中央接入服务器或管理员设备进行通信。当用户请求接入锁时，可移除无线按钮将请求传送到网络设备、管理员设备或中央接入服务器。可移除无线按钮被配置为直接与中央接入服务器和管理员设备通信，或间接通过网络设备进行通信。该按钮可以从锁芯分离并且对接在充电站上。在一些实施例中，可移除无线按钮包括确定门是打开还是关闭的惯性模块运动传感器。



CN 107889536 B

1.一种用于提供冗余接入控制的锁,包括:

硬件处理器;

适于匹配门的标准规格槽的锁芯,所述锁芯包括用于接合门栓的凸轮;

用于接合所述凸轮以解锁所述门栓的按钮,所述按钮包括电源和用于接收认证信息的多个冗余接入信道,所述冗余接入信道包括用于接收生物特征信息的生物特征扫描器、密码小键盘和无线收发机,所述无线收发机配置为与移动设备以及以下之一近实时地进行通信:1)网络设备,2)中央接入服务器,以及3)管理员设备;

可再充电电源,其中,所述按钮是用于解锁所述门栓并为所述可再充电电源通电的自由旋转的按钮,通过所述按钮的运动生成的旋转能量被转换成电能并被储存在所述可再充电电源中,并且当所述按钮被旋转以解锁所述门栓时,所述按钮生成给所述可再充电电源供电的电能:

其中所述硬件处理器配置为:

基于从所述移动设备、网络设备、中央接入服务器或管理员设备接收的通信来验证从所述密码小键盘、生物特征扫描器或移动设备接收的认证信息,

当用户通过所述多个冗余接入信道中的第一信道被认证时,解锁所述门栓,并且

当用户不能通过所述第一信道打开所述锁时,允许通过所述多个冗余接入信道中的第二信道进行接入,以及

其中所述按钮是可移除的,并且所述按钮还包括再充电接口和用于存储接入信息的存储介质,其中所述再充电接口被配置为耦合到电源插座或再充电站以对所述按钮再充电,并且其中所述存储介质被配置为当所述按钮被再充电时发送所述接入信息,以及所述按钮被配置为在输入有效凭证时被移除。

2.根据权利要求1所述的锁,还包括被配置为创建蜂窝宽带连接并且近实时地与管理员设备或中央接入服务器进行通信的无线调制解调器。

3.根据权利要求1所述的锁,还包括被配置为创建短距离无线连接并且近实时地与管理员设备或中央接入服务器进行通信的无线调制解调器。

4.根据权利要求2所述的锁,其中所述锁被配置为通过所述蜂窝宽带连接从所述中央接入服务器或所述管理员设备接收指令,以基于所述用户的生物特征扫描、密码或移动设备IMEI来阻止用户的接入。

5.根据权利要求1所述的锁,其中所述锁被配置为:

接收令牌、生物特征扫描或密码,

基于一组可配置规则发送对所述锁的接入请求,并且

近实时地从所述管理员设备或中央接入服务器接收准许或拒绝所述接入请求的指令。

6.根据权利要求1所述的锁,其中所述按钮包括惯性模块,所述惯性模块被配置为确定指示门是已经被打开还是关闭的门状态,并且将所述门状态近实时地传送到所述管理员设备或中央接入服务器。

7.根据权利要求1所述的锁,其中所述锁被配置为确定指示所述门栓是处于锁定位置还是解锁位置的门栓状态,并且将所述门栓状态近实时地传送到所述管理员设备或中央接入服务器。

8.根据权利要求1所述的锁,其中所述按钮是设置在所述门的内表面上的第一按钮并

且包括电源，并且其中所述锁还包括耦合到所述锁芯的第二按钮，所述第二按钮设置在所述门的外表面上且由所述第一按钮的电源供电。

9.根据权利要求1所述的锁，其中所述按钮还包括被配置为从外部设备接收电力并且将接入信息输送到所述外部设备的I/O端口。

10.一种用于控制具有冗余接入信道的锁的系统，所述系统包括：

根据权利要求1所述的用于提供冗余接入控制的锁；以及

网络设备，其中所述锁通过短距离无线连接耦合到所述网络设备，并且所述网络设备通过网络连接耦合到所述管理员设备或中央接入服务器。

11.根据权利要求10所述的系统，其中所述网络设备被配置为从所述锁接收令牌、生物特征扫描或密码，并将所述令牌、生物特征扫描或密码中继到所述管理员设备或中央接入服务器。

12.根据权利要求10所述的系统，其中所述网络设备被配置为从所述中央接入服务器或管理员设备接收指令，以基于所述用户的生物特征扫描、密码或移动设备IMEI阻止用户的接入。

13.根据权利要求10所述的系统，还包括通过短距离无线连接耦合到所述网络设备的设备互连集线器，其中所述网络设备被配置为在触发事件时与所述设备互连集线器通信。

14.一种用于控制对锁的接入的方法，所述锁包括硬件处理器，包括用于接合门栓的凸轮的锁芯，用于接合所述凸轮以解锁所述门栓的按钮，和可再充电电源，所述按钮包括电源、再充电接口、用于存储接入信息的存储介质、多个冗余接入信道和配置为通过短距离无线连接与网络设备通信的无线收发机，所述方法包括以下步骤：

通过所述短距离无线连接从所述锁接收用户认证信息，所述认证信息用于获得对所述多个冗余接入信道中的第一冗余接入信道的接入，所述多个冗余接入信道包括生物特征扫描、密码或令牌；

通过网络连接将所述认证信息发送到管理员设备或中央接入服务器，以便基于一组可配置规则进行验证；

在所述管理员设备或中央接入服务器处验证所述认证信息；

从所述管理员设备或中央接入服务器接收指令以准许或拒绝对用户的接入；并且

向所述锁发送准许或拒绝对用户的接入的指令，并且当所述指令准许对用户的接入时，解锁所述门栓，

当用户不能通过所述第一冗余接入信道打开所述锁时，允许通过所述多个冗余接入信道中的第二信道进行接入，

在所述按钮处接收有效凭证的输入，其使得所述按钮被移除，以及

将所述再充电接口与电源插座或再充电站耦合以对所述按钮再充电，并且当所述再充电接口与电源插座或再充电站耦合时从所述存储介质发送所述接入信息；

其中，所述按钮是用于解锁所述门栓并为所述可再充电电源通电的自由旋转的按钮，通过所述按钮的运动生成的旋转能量被转换成电能并被储存在所述可再充电电源中，并且当所述按钮被旋转以解锁所述门栓时，所述按钮生成给所述可再充电电源供电的电能。

15.根据权利要求14所述的方法，还包括：

登记触发事件；以及

基于所述触发事件向设备互连集线器发送指令。

16.根据权利要求14所述的方法，还包括基于由所述锁保有的接入信息来确定用户模式。

17.一种用于控制对锁的接入的方法，所述锁包括硬件处理器，包括用于接合门栓的凸轮的锁芯，用于接合所述凸轮以解锁所述门栓的按钮，和可再充电电源，所述按钮包括电源、再充电接口、用于存储接入信息的存储介质、多个冗余接入信道和配置为创建用于直接与管理员设备或中央接入服务器通信的蜂窝宽带连接的无线收发机，所述方法包括以下步骤：接收用于获得对所述多个冗余接入信道中的第一冗余接入信道的接入的用户认证信息，所述多个冗余接入信道包括生物特征扫描、密码或令牌；将所述认证信息发送到管理员设备或中央接入服务器以基于一组可配置规则通过所述蜂窝宽带连接进行验证；在所述管理员设备或中央接入服务器处验证所述认证信息，从所述管理员设备或中央接入服务器接收准许或拒绝对用户的接入的指令；以及基于准许或拒绝对用户的接入的决定，使凸轮接合以打开或关闭所述锁的门栓，并且当所述指令准许对用户的接入时，打开所述门栓，当用户不能通过所述第一冗余接入信道打开所述锁时，允许通过所述多个冗余接入信道中的第二信道进行接入，在所述按钮处接收有效凭证的输入，其使得所述按钮被移除，以及将所述按钮的再充电接口与电源插座或再充电站耦合以对所述按钮再充电，并且当所述再充电接口与电源插座或再充电站耦合时从所述存储介质发送所述接入信息；其中，所述按钮是用于解锁所述门栓并为所述可再充电电源通电的自由旋转的按钮，通过所述按钮的运动生成的旋转能量被转换成电能并被储存在所述可再充电电源中，并且当所述按钮被旋转以解锁所述门栓时，所述按钮生成给所述可再充电电源供电的电能。

用于冗余接入控制的锁和方法

[0001] 相关申请的交叉引用

[0002] 本申请要求于2016年5月5日提交的美国专利申请第15/147,759号的优先权，该美国专利申请要求于2015年7月6日提交的美国临时专利申请第62/189,193号的优先权，这两个专利申请全部内容通过引用并入本文。本申请涉及于2016年3月3日提交的美国专利申请第15/060,327号，其全部内容也通过引用并入本文。

技术领域

[0003] 本发明涉及锁和移动设备，更具体地，涉及使用移动设备、接入控制冗余信道和可移除无线锁按钮控制对锁的接入的系统和方法。

背景技术

[0004] 使用机械或机电钥匙和锁的进入控制系统持续遭受若干缺点。具体而言，机械锁和钥匙不能针对盗窃、丢失、非法进入或不期望的复制提供强大的防护。例如，如果钥匙丢失或被盗，锁通常会被替换。机械锁和钥匙也不提供关于钥匙如何或何时被使用的信息-或者如果有的话该信息也不是近实时的。这种类型的信息对于个人来说可能是非常需要的，并且对于某些企业来说可能是关键的。使用电子锁和钥匙系统提供接入信息的系统通常硬件连接到门框中。此外，硬件连接的解决方案完全依赖于直接或替代形式的电源和数据连接以高效地运行。硬件连接系统通常安装成本高，在温度范围变化很大的室外环境中表现不佳，并且与通用系统(诸如欧规锁芯(Europrofile cylinder))不兼容。此外，大多数传统的机械锁系统使用的钥匙仅可用于进入一个门，因此，需要通过多个锁的用户由于不得不携带一串用于其相应锁的不同钥匙而不方便。

[0005] 移动设备的无线通信能力(诸如例如NFC和蓝牙之类的)提供了改善使用机械或机电钥匙的接入控制系统的机遇。具体地说，移动设备的近场通信(NFC)、蓝牙或类似的无线能力可以通过使用移动设备作为电子密钥来适配作进入控制系统。此外，在一些移动设备上近实时地传送接入数据的能力提供了传递关于密钥如何以及何时被使用以及锁被打开的信息的机会。

[0006] 然而，将移动设备集成到接入控制系统中仍然存在若干缺点。与机械锁和钥匙系统一样，移动设备不能对于盗窃和非法进入提供强大的防护。此外，移动设备通常依赖于电池作为其电源，在用户打开锁之前电池经常会耗尽电量。此外，对于一些企业来说，在其所有资产中部署移动设备可能是昂贵和不切实际的。此外，无论移动设备是否耗尽电量，在范围之外，还是由于其它原因不可用，用户可能无法接入锁或锁中存储的信息。

[0007] 另外，为了将移动设备集成到接入控制系统中，锁通常配备有NFC和无线通信设备。然而，这些设备需要连续可靠的电源。虽然电池电源适用于NFC或无线设备(如移动设备)，但是它们可能会意外耗尽电量或遭受其他故障，使用户无法通过移动设备打开锁。

[0008] 因此，需要一种作为机械锁的安全可靠的替代方案的接入控制系统，以及在近实时地提供使用信息的同时提供冗余接入信道，并在故障或放电的情况下提供冗余的电力供

应的移动设备。接入控制系统应易于安装，减少使用的有线连接数量，并可在长时间段内独立地运行。接入控制系统的冗余信道应允许能或不能使用普通电话、智能手机、平板电脑和类似移动设备的用户接入锁。此外，接入控制系统应允许锁与网络以及连接到网络的用户和设备直接且实时地通信。

发明内容

[0009] 在各种实施例中，本发明提供了用于控制和监视接入控制系统的系统、方法和装置。根据本发明的一些实施例，接入控制系统包括提供冗余接入控制的智能锁。智能锁包括存储介质、电源、硬件处理器、具有接合门栓的凸轮的锁芯以及接合凸轮以解锁门栓的按钮。

[0010] 按钮包括用于接收认证信息的多个冗余接入信道。冗余接入信道可以包括用于接收生物特征信息的生物特征扫描器、密码小键盘和/或用于从移动设备接收令牌并向移动设备发送应答的无线收发机。

[0011] 智能锁被配置为基于由管理员确定的一组规则来验证从密码小键盘、生物特征扫描器和/或移动设备接收的认证信息，并且如果用户通过多个冗余接入信道中的第一信道被认证，则解锁门栓。如果用户无法通过第一信道打开智能锁，则启用智能锁以允许通过多个冗余接入信道中的第二信道接入。以这种方式，当用户不再能够使用第一信道接入智能锁时，用户可以使用第二信道打开锁。

[0012] 接入控制系统可以包括一个或多个智能锁。这些系统可以由请求接入智能锁的用户接入，并由限制对智能锁的接入的主人或管理员控制。在一些实施例中，用户可以接入，并且主人或管理员可以近实时地从其各自的移动设备控制对智能锁的接入。主人和管理员可以使用移动设备配置控制用户如何和何时打开智能锁的规则和接入权限。以这种方式，可以提供允许主人和管理员近实时地控制和监视用户的接入控制系统，而无需将硬件连接的互联网或数据连接安装到门或锁上。由于锁芯适于配合标准槽，因此门框和锁系统不需要修改或重装。

[0013] 在本发明的一些方面，主人或管理员可以配置限制用户如何接入智能锁的规则和接入权限。接入权限指定用户可以接入哪些锁，并且可配置规则指定在打开智能锁之前必须满足的条件。因此，规则允许主人或管理员根据位置和时间来限制用户的接入。以这种方式，可以使主人或管理员精确地控制用户如何打开智能锁。

[0014] 每次尝试打开智能锁时，主人和管理员可能要求用户请求密码或令牌。当用户提交请求时，主人或管理员可以近实时地接收请求，并确定是否授予用户接入权限。主人或管理员可能要求用户提供另外的认证信息，例如口令，以确保用户的身份。如果主人或管理员确定授予用户接入权限，则将令牌或密码近实时地发送给用户。在一些实施例中，可以基于触发事件发送请求。因此，主人或管理员可以根据具体情况控制用户的接入。

[0015] 密码可以是固定的或动态的。动态密码可使主人或管理员能够授予用户对锁的一次性使用接入或限时接入。密码可以从移动设备无线地提供给锁，或者手动输入到小键盘上。因此，即使用户的移动设备不可用，用户也能够利用密码接入锁。

[0016] 在本发明的一些实施例中，智能锁的无线收发机被配置为直接且近实时地向移动设备以及网络设备、控制接入服务器或管理员设备进行通信。然后，锁可以从网络设备、控

制接入服务器或管理员设备接收指示锁准许或拒绝对用户的接入的通信。

[0017] 根据本发明的一些实施例，智能锁包括被配置为创建蜂窝宽带连接并且近实时地与管理员设备或中央接入服务器通信的无线调制解调器。当锁接收到令牌、生物特征扫描或密码时，它可以基于一组可配置规则来发送接入锁的请求。然后，锁可以近实时地从管理员设备或中央接入服务器接收准许或拒绝接入请求的指令。以这种方式，如果用户的移动设备不能与管理员设备或中央接入服务器通信，则该锁可以自己建立到管理员设备或中央接入服务器的连接。因此，锁可以在不依赖于用户的移动设备来中继通信的情况下与管理员设备或中央接入服务器进行通信。

[0018] 在本发明的其它实施例中，智能锁还可以被配置为与将通信中继到管理员设备或中央接入服务器的网络设备进行通信。网络设备可以是使用近场无线发射机或无线LAN来建立短距离无线连接的无线接收机、路由器、中继器或类似设备。因此，智能锁可以类似地创建连接以与管理员设备或中央接入服务器通信，而不依赖于用户的移动设备来中继通信。

[0019] 智能锁可以包括惯性模块。该惯性模块被配置为确定指示门是否已经打开或关闭的门状态。锁可以类似地被配置为确定指示门栓的锁定或解锁位置的门栓状态。该锁可以近实时地将门状态和门栓状态传送到管理员设备或中央接入服务器。因此，管理员设备或中央接入服务器可以确定门是否已经被打开、关闭、锁定或解锁。

[0020] 根据本发明的一些实施例，智能锁的按钮可以是可移除的和可再充电的。该按钮可以包括与再充电站的再充电接口相匹配的再充电接口。当按钮的电源不足时，用户可以取出按钮，并用再充电站对按钮进行再充电。在本发明的另外的实施例中，该按钮可以包括允许用户从例如外部设备或再充电站为该按钮供电的I/O端口。I/O端口还允许用户获取存储在按钮上的接入信息。因此，当按钮在再充电站上进行再充电时，充电按钮可以通过I/O端口获取存储在按钮上的接入信息。在一些实施例中，再充电站耦合到使其能够将接入信息传送到管理员设备或中央接入服务器的网络连接。

附图说明

[0021] 参考以下详细描述和附图，可以更好地理解本发明的目的和特征。

[0022] 图1A、1B、1C和1D示出了根据本发明的实施例的接入控制系统。

[0023] 图2A、2B、2C和2D示出了根据本发明实施例的用于接入控制系统的智能锁。

[0024] 图3示出了根据本发明的实施例的具有可再充电电源的智能锁。

[0025] 图4示出了根据本发明的实施例的用于打开智能锁的过程。

[0026] 图5示出了根据本发明的实施例的在接入控制系统中登记触发事件的过程。

[0027] 图6示出了根据本发明的实施例的接入控制系统中用于控制对智能锁的接入的过程。

[0028] 图7A、7B、7C、7D和7E示出了根据本发明的实施例的接入控制系统中用于控制对智能锁的接入的接口。

[0029] 图8A、8B、8C、8D、8E和8F示出了根据本发明的实施例的接入控制系统中用于控制智能锁的接口。

[0030] 图9A、9B和9C示出了根据本发明的实施例的接入控制系统中用于接入智能锁的用

户接口。

具体实施方式

[0031] 本发明的实施例包括使得用户能够使用冗余接入信道打开锁并允许主人或管理员近实时地控制用户的接入的系统、方法和装置。

[0032] 在图1A和1B中示出了在向用户提供冗余的接入信道的同时近实时地传送使用信息的示例性接入控制系统。该系统包括一个或多个智能锁104、中央接入服务器105，以及用于接入和控制智能锁的设备101，102和103。用户通过一个或多个接入信道打开智能锁104，如下面更详细描述的。主人和管理员控制用户如何从主人设备101或管理员设备102接入智能锁104。用户可以与主人、管理员通信，并且从用户设备103打开智能锁。用户还可以手动地打开智能锁，而没有对用户设备103的任何需要。中央接入服务器105近实时地中继和存储在用户与主人或管理员之间交换的信息。值得注意的是，“近实时”通信是可能表现为实时或基本上实时发生、但是由于网络基础设施而导致经历轻微的、不明显的或不显著的延迟的通信。当用户不能再通过其中一个接入信道打开智能锁，例如因为接入信道不可用或变得无法操作，用户可以通过其他可用的接入信道打开智能锁。因此，接入控制系统100使得用户能够使用冗余接入信道打开智能锁，并允许主人或管理员近实时地控制用户的接入。

[0033] 主人设备101和管理员设备102为寻求获得对一个或多个智能锁104的接入的用户创建和分配规则和接入权限。接入权限识别每个用户被授权打开的智能锁104。规则添加在允许用户打开智能锁104之前必须满足的条件。例如，接入权限可以由主人设备101或管理员设备102配置为指定用户可以打开的一组智能锁104，而规则指定用户在什么日期和时间被允许打开特定的智能锁。

[0034] 如图1B所示，主人设备101和管理员设备102还被配置为指定用户可以使用哪些接入信道来提供认证信息以打开智能锁104。如下面更详细地解释的，接入信道可以例如为：将生物特征信息扫描到生物特征扫描器114中，在小键盘115上输入密码，或从移动设备116无线地发送令牌。智能锁可以将任何或所有接入信道的组合提供给用户。例如，用于常规或默认使用的第一接入信道可以是从用户的移动设备116无线地传送令牌，并且第二接入信道和第三接入信道可以分别是生物特征扫描器114和密码小键盘115，其在第一接入信道变得对用户不可用的情况下使用。

[0035] 主人设备101、管理员设备102或用户设备103可以是移动设备、软件服务或软件应用。移动设备可以是例如智能电话、平板电脑或手持设备。移动设备包括触摸屏显示器107、存储介质108和处理器109。在一些实施例中，移动设备包括用于接收和发送RFID、NFC或蓝牙信号，或者通过移动设备的蜂窝或互联网连接的无线收发机110。

[0036] 中央接入服务器105可以是基于云的服务器，并且可以连接到远程服务器106。远程服务器106可以包括具有接收用户呼叫和接入请求的代理的呼叫中心。

[0037] 在本发明的一些实施例中，移动设备包括NFC元件111，其可以是配备有NFC发射机的SIM卡或SD卡。可将具有NFC功能的SD卡放置在移动设备的SD卡插槽中，为智能手机提供NFC通信能力。类似地，可将具有NFC功能的SIM卡放置在移动设备的SIM卡插槽中，为智能手机提供NFC通信能力。

[0038] 如图1A所示，接入控制系统中的个体可以具有不同的角色。例如，个体可能是主人、管理员或用户。主人可以添加、删除和配置管理员或用户的接入权限。管理员可以类似地添加、删除和配置用户的接入权限。用户是寻求进入由智能锁保护的场地的个人。可以为每个用户或管理员，或者在更普遍的级别为一组用户或管理员，配置个体的接入权限。类似地，可以向用户或管理员授予对特定的智能锁或一组智能锁的接入。

[0039] 例如，在商业环境下的接入控制系统中，主人设备101或管理员设备102可以由希望控制其员工如何和何时进入公司内的区域的主管或管理者来操作。业务经理可以指定一名主管作为管理员，该管理员可以进一步将一组员工指定为对特定一组智能锁有接入权的用户。作为另一示例，在住宅环境下，主人设备101或管理员设备102可以由家长操作以控制人员进入其房屋不同区域的接入权并监视人员进入其房屋不同区域的接入信息。指定自己作为主人的家长可以将他们的保姆指定为管理员并将他们的孩子指定为用户，并规定保姆和孩子可以进入房屋的哪些区域以及他们如何以及何时可以进入这些区域。如下面更详细描述的，主管或家长可以接收关于雇员、保姆或孩子如何以及何时尝试进入由智能锁104控制的场地的警报或报告。

[0040] 接入控制系统的主人或管理员使用一组规则112和接入权限113来配置用户如何打开智能锁。接入权限113识别接入控制系统中的每个个体或个体组，以及接入控制系统中的每个智能锁或智能锁组。接入权限113还将每个个体与智能锁相关联。规则集12指定了何种接入信道可以用于打开智能锁，以及(如果有)需要何种条件才能使个体打开智能锁。例如，指定自己作为主人的家长可以配置保姆的接入权限和规则，使得他们可以使用密码或生物特征扫描来打开智能锁。这些规则可以进一步被配置有条件，使得保姆只能在一周中的某些天或者家长批准每次接入请求之后才能打开智能锁。

[0041] 接入权限和规则可以存储在中央接入服务器、智能锁、用户、管理员或主人的移动设备中。如下面更详细说明的，主人或管理员可以从主人设备101、管理员设备102或中央接入服务器105创建、修改或删除接入权限和规则。当主人或管理员创建、修改或删除接入权限或规则时，接入权限或规则可以被传送到用户的移动设备或中央接入服务器。然后，用户的移动设备随后可以将接入权限或规则作为令牌的一部分发送到智能锁。当用户尝试打开智能锁时，可以从移动设备或智能锁检查接入权限和规则。例如，如果用户提供密码或生物特征扫描，则智能锁可以检查接入权限和规则以确定用户是否被授权在给定日期或时间打开智能锁。作为另一示例，在将令牌发送到智能锁之前，用户的移动设备可以检查接入权限和规则以确定用户是否被授权打开特定的智能锁。如果用户不具有授权，则移动设备将不发送令牌给智能锁。在本发明的一些实施例中，可以从主人设备101、管理员设备102或中央接入服务器105检查接入权限和规则。

[0042] 可以安装智能锁以保护场地内的特定区域或房间，从而使得主人或管理员能够精确地控制个体可以获得何处的进入权限。例如，在手机信号塔中，智能锁可以安装在设施的前门，储藏室的门和柜子的门上，这些地方中通常是盗窃目标的电池、铜缆、电子设备和其他资产得以保全。然后，公司经理(例如，主人)可以准许某些雇员(例如，用户)对设施的进入，同时将对储存室和柜门的进入限制为选定的少数员工。如上所述，公司经理可以进一步配置规则以规定员工如何接入智能锁，以及(如果有的话)何种条件使雇员获得接入权限。

[0043] 作为另一示例，场地内的区域可以是例如地下室、后院、卧室、前大门、健身中心或

车库。因此，在住宅环境中，家长可以使保姆进入地下室、后院或家长的卧室，但只能在保姆照顾婴儿的特定时间段期间。如下所述，家长可以进一步配置规则以授予保姆附条件的进入权限，其需要保姆在其每次寻求接入智能锁时请求许可。家长可以进一步配置接入权限和规则以授予孩子在加强的限制下进入家中不同的区域或房间的权限。例如，家长可以配置接入权限和规则来拒绝孩子进入房屋中例如地下室的房间，或限制在一天的特定时间段内进入诸如健身中心的区域。家长可以进一步配置规则以规定孩子可以使用哪些接入信道来进入该区域，例如使用孩子的指纹来进入后院。

[0044] 根据本发明的一些实施例，用户通过从用户的移动设备到智能锁的无线通信116来打开一个或多个智能锁104。通过使用用户的移动设备的无线功能，智能锁104可以被链接到中央接入服务器105，而没有两者之间的直接连接。以这种方式，可以远程地控制对智能锁104的接入，而不需要在门框或锁上实现硬件连接系统。

[0045] 如上所述，智能锁104可以通过将令牌从用户的移动设备无线地发送到智能锁104来打开。令牌包含包括字母、数字、符号或其任何组合的密码。密码可以是动态的或固定的，如下面更详细地讨论的。智能锁104基于由主人或管理员确定的接入权限和规则并且通过将接收到的密码与由智能锁104中存储的进程产生的密码进行比较来验证令牌。如果接收到的密码与进程产生的密码相匹配，则智能锁104将接受令牌。基于接入权限和规则以及该令牌是否与存储的进程产生的令牌相匹配，智能锁104向用户的移动设备103传送该令牌是否被验证。然后可以将该信息从用户移动设备103发送到中央接入服务器105，在中央接入服务器中该信息可以作为通知或警报被中继到主人设备101或管理员设备102。

[0046] 主人设备101和管理员设备102被配置为规定用户是否可以使用用户的移动设备的无线能力接入智能锁104，以及用户具有哪些接入权限。例如，主人设备101和管理员设备102可以规定用户的对特定智能锁104或智能锁104组的接入权限是固定的或附条件的。

[0047] 附条件的接入权限允许主人或管理员批准用户打开智能锁104的每次尝试。例如，当具有附条件的接入权限的用户尝试接入智能锁104或智能锁104组时，系统将警告主人设备101或管理员设备102用户103正在试图接入智能锁104，并且近实时地请求主人设备101或管理员设备102准许用户对智能锁104的接入。用户然后可以确定是否允许或拒绝用户接入。该确定可以基于附加条件或验证步骤。例如，主人或管理员可以请求用户提供证明用户身份或真实性的标识信息，诸如例如附加口令。作为另一示例，管理员的主人可以拒绝用户接入，因为用户不应接入该特定智能锁104，或者不应在该特定日期或时间接入。如果主人或管理员确定用户对智能锁104的接入应被准许，则主人设备101或管理员设备102然后可以向用户提供如下面更详细描述的令牌。如果主人或管理员确定用户对智能锁104的接入应被拒绝，则主人设备101或管理员设备102不向用户提供令牌，并且用户将无法打开智能锁104。以此方式，主人设备101或管理员设备102可以近实时地允许或拒绝对智能锁104的接入。在一些实施例中，当主人或管理员确定是否准许或拒绝用户接入时，主人设备101或管理员设备102向用户发送警报，通知用户他们的接入请求已被准许或拒绝。

[0048] 固定接入权限允许用户在没有首先接收到来自主人设备101或管理员设备102的批准的情况下获得对智能锁104的接入。例如，用户可以被授予以不受限制的方式打开特定智能锁104的固定接入权限。这样的固定接入可以通过固定密码提供，例如用户可以在智能锁104的小键盘上输入的固定密码。然后，用户可以使用固定密码打开智能锁104，而无需首

先请求主人设备101或管理员设备102的批准。在一些实施例中，当具有固定接入权限的用户已经接入或尝试接入智能锁104时，用户的移动设备103仍然可以通知主人设备101或管理员设备102。例如，在用户在智能锁小键盘上输入固定密码之后，智能锁可以向用户的移动设备通信它接收到有效的固定密码并解锁智能锁。然后，用户的移动设备可以近实时地通知主人设备101、管理员设备102或中央接入服务器105用户接入并解锁智能锁104。

[0049] 主人设备101和管理员设备102还可以用于允许用户使用在小键盘115上输入的密码或生物特征扫描114打开一个或多个智能锁104。这些接入信道使得用户能够获得对智能锁104的接入而不使用移动设备，因为如下面更详细描述的，密码或生物特征扫描可以由用户手动输入。以这种方式，用户可以在他们不拥有移动设备、或者他们的移动设备丢失、损坏或者由于其它原因无法将令牌无线发送到智能锁104的情况下获得对智能锁104的接入。因此，根据本发明的一些实施例，用于输入密码的小键盘或生物特征扫描用作向用户提供对智能锁104的接入的冗余接入信道。在本发明的其它实施例中，用于输入密码或生物特征扫描的小键盘可以用作主要或默认接入信道，而从用户的移动设备到智能锁104无线通信可以用作冗余接入信道。在本发明的另外的实施例中，可能要求用户使用替代接入信道的组合来认证自身。例如，可能要求用户在授予对锁的接入权之前提供动态密码和指纹的组合。

[0050] 如上所述，令牌可以包括可以从用户的移动设备103无线地发送到智能锁104的密码。如下面更详细地描述的，密码也可以显示在用户设备上，使得用户可以手动将其输入到智能锁104的小键盘上。智能锁04通过将输入的密码与存储在智能锁404上的进程所产生的密码进行比较来验证固定密码。如果该进程产生匹配的密码，则智能锁104将授予用户接入权限。

[0051] 在本发明的一些实施例中，密码可以是由代码生成系统(CGS)生成的动态密码。动态密码是中央接入服务器根据请求而生成的唯一的、单次使用的、限时的或一次性密码。密码部分基于请求密码的时间。

[0052] 根据本发明的一些实施例，提供给用户的密码的生成基于关于用户的移动设备的唯一信息和请求或正在生成密码的时间。对于移动设备，密码可以基于例如国际移动设备标识(“IMEI”)、移动设备的网络ID或两个ID的组合，以及从移动设备发送请求的时间。

[0053] 可替代地，密码可以是固定的。固定密码不会更改或过期，可以被使用不止一次，并且可以在没有来自主人或管理员的请求的情况下获得。希望阻止固定密码被泄漏的主人或管理员可以要求固定的密码与其他信息或生物特征扫描结合使用。

[0054] 用户可以通过联系主人或管理员来请求动态的或固定的密码。例如，用户的移动设备103可以包括移动应用，其允许用户通过移动设备的蜂窝数据、WiFi或NFC/蓝牙连接向主人设备101、管理员设备102或中央接入服务器105发送密码请求。作为另一示例，用户可以通过从用户的移动设备向主人、管理员或中央接入服务器代理发起语音呼叫或者发送文本消息来提交请求。以这种方式，即使当移动设备不能连接到互联网或者没有配备数据或互联网连接时，用户也可以发送请求。

[0055] 在本发明的一些实施例中，智能锁104可以通过提供用户的生物特征扫描来打开。如下面更详细地描述的，智能锁04包括存储介质201，其可以存储被授权接入锁的每个用户的生物特征数据。生物特征数据可以包括例如每个用户的指纹。当用户接收到生物特征扫

描时，智能锁104将扫描与存储在智能锁104中的生物特征数据进行比较。如果扫描与所存储的生物特征数据匹配，则智能锁将准许用户接入。当生物特征扫描器用作冗余接入信道时，如果例如用户没有或丢失其移动设备并且不能获得令牌或密码，则用户可以提供生物特征扫描。

[0056] 图1C示出了根据本发明的一些实施例，智能锁104耦合到主人设备101、管理员设备102或中央接入服务器106，从而绕过移动设备。例如，智能锁104可以耦合到网络设备117，网络设备117将通信中继到主人设备101、管理员设备102或中央接入服务器106。网络设备117可以是例如无线接收机、路由器、中继器或类似设备。作为另一示例，智能锁104可以通过蜂窝宽带连接直接与主人设备101、管理员设备102或中央接入服务器106进行双向通信，如下面更详细描述的。

[0057] 在如图1C所示智能锁104与网络设备117通信的配置中，智能锁104可以使用近场无线发射机或无线LAN来建立短距离无线连接。可以使用例如蓝牙、NFC、ZigBee或类似的短距离无线网络技术来建立连接。例如，网络设备117可以是家中的无线中继器、扩展器或路由器，并且使用蓝牙来与智能锁通信。然后，网络设备117可以使用诸如因特网、以太网或类似连接的网络连接耦合到主人设备、管理员设备或中央接入服务器。然后，网络设备117可以近实时地中继从智能锁到主人设备，管理员设备或中央接入服务器的通信。因此，即使当用户的智能手机或移动设备被盗或不可操作时，智能锁也能够近实时地与主人设备、管理员设备或中央接入服务器进行通信。

[0058] 在本发明的一些实施例中，智能锁可以包括直接与中央服务器或管理员通信的无线发射机，如图1D所示。例如，智能锁104可以包括蜂窝宽带或广域网连接，其使得按钮能够直接与主人设备101、管理员设备102或中央接入服务器106进行通信。锁可以包括用于建立蜂窝宽带连接并且以近实时的方式传送信息的无线调制解调器。例如，调制解调器可以是嵌入在锁中的芯片组上的Intel XMM 62553G调制解调器。在另外的实施例中，调制解调器可以是提供对蜂窝网络的接入的USB加密狗、数据卡或类似设备，并且可以通过I/O端口耦合到锁，如下面更详细描述的。蜂窝网络可以是例如GSM，GPRS，EDGE，UMTS，HSDPA，HSPA，HSPA+，CDMA，LTE或类似的蜂窝网络。

[0059] 令智能锁能够与主人设备、管理员设备或中央接入服务器通信提供了对用户接入智能锁的附加控制。例如，智能锁可以被配置为在每次用户尝试获得对智能锁的接入权时向主人设备或管理员设备发送获得批准的请求。因此，即使用户尝试使用密码或生物特征扫描来获取接入权限时，主人或管理员也可以批准每次接入请求。

[0060] 作为另一示例，智能锁可以使用到主人设备、管理员设备或中央接入服务器的连接来核实用户是否被授权打开智能锁。具体来说，在接收到认证信息之后，智能锁可以与主人设备、管理员设备或中央接入服务器通信，主人设备、管理员设备或中央接入服务器检查一组可配置规则以核实用户是否被授权接入智能锁。

[0061] 在本发明的另一方面，主人设备、管理员设备或中央接入服务器可以将指令传送到智能锁以执行某些功能或过程。例如，如果中央接入服务器确定智能锁的门栓被解锁，则中央服务器可以指示智能锁锁定门栓。以这种方式，如果管理员或用户离开家，而不记得其是否锁门，则管理员或用户可以确认门是否未上锁，并且如果确实如此，则将其远程上锁。在其他实施例中，主人设备、管理员设备或中央接入服务器可以将指令传送到智能锁，以阻

止从某些设备接收的通信或从某些用户接收的生物特征。例如，如果用户的移动设备已被报告为丢失或被盗，则主人设备、管理员设备或中央接入服务器可以指示智能锁阻止从该特定移动设备接收到的任何通信。类似地，主人设备、管理员设备或中央接入服务器可以向智能锁发送特定用户将不再被允许使用其生物特征扫描来解锁智能锁，并且报告从该用户接收的任何这样的生物特征扫描的指令。

[0062] 根据本发明的一些实施例，按钮包括用于检测和测量门的移动和位置的惯性模块。惯性模块可以包括用于检测和测量移动和/或位置的传感器组合，例如基于MEMS的加速度计、陀螺仪和/或磁力计。基于MEMS的加速度计可以是1轴，2轴或3轴加速度计，并且测量可以包括例如门在这些轴上的速度和加速度。可以对由加速度计提供的测量值进行滤波和分析，以确定运动是否与门的打开或关闭相关。可以使用的其它传感器可以包括磁传感器，例如磁性开关，其响应于其磁场的变化而产生测量值。也可以使用电位计来产生对应于门框铰链的角移动和位置的信号。其他实施例可以包括在门打开或关闭时测量光或声波的反射的光学或超声波传感器。

[0063] 由惯性模块的传感器进行的测量用于跟踪位置和门移动的变化，使按钮能够确定门是打开还是关闭。在一些实施例中，按钮可以通过将传感器测量值与与门的打开和关闭相关联的已知加速度和/或移动特征进行比较来确定门是打开还是关闭。例如，关闭门的移动的特征在于其加速度的变化；如果加速度急剧增加(即用户推门)，随后突然减小(即，门接触门框并且关闭)，则按钮可以确定门被关闭。作为另一个示例，关门的移动可以以其速度表征；如果速度或加速度达到最大阈值，则可以确定门已经达到使得其最终将关闭的速率或速度。类似地，如果门的速度或加速度从未达到最小阈值，则可以确定门没有被足以关闭的力推动。该按钮可被配置为跟踪门在什么时间被打开或关闭。例如，按钮可以通过在智能锁的存储介质中保持日志来记录门在何时被打开或关闭。

[0064] 在本发明的另外的方面，这些传感器可以用于检测锁具锁芯的门栓是否已经旋转，从而指示用户是否已经锁定或解锁了门。例如，加速度计可用于检测使门栓延伸到门榫内的按钮的旋转。该按钮还可以被配置为跟踪凸轮在什么时间被接合来锁定或解锁门栓。在本发明的一些实施例中，按钮可以包括门栓的锁定或解锁状态，以确认门是被打开还是被关闭。例如，如果按钮检测到门被关闭，则按钮可以通过确定门栓是否从解锁状态变为锁定状态(其指示门被关闭并被锁定)来确认门已经关闭。

[0065] 在本发明的一些实施例中，该按钮可将门打开、关闭、锁定还是解锁传送到网络设备、管理员设备、主人设备或中央接入服务器。以这种方式，用户可以远程确定他们的门是打开还是关闭。

[0066] 图2A和图2B示出了根据本发明的一些实施例的智能锁。智能锁包括存储介质201、电源202、硬件处理器203、锁芯204和按钮205。智能锁还可以包括无线收发机206、密码小键盘207和生物特征扫描器208。锁芯包括接合门栓(未示出)的凸轮209。用户向智能锁提供认证信息，认证信息由硬件处理器203和存储介质201验证。认证信息可以是例如用户扫描的指纹、输入到小键盘上的密码、或从用户设备无线发送的令牌。当智能锁验证认证信息时，按钮205接合凸轮205，该凸轮解锁门栓。存储介质201存储用于验证认证信息，保持接入事件和智能锁使用的日志以及标识智能锁的信息和数据。例如，存储介质可以存储被授权打开锁的用户的资料数据或标识智能锁的唯一标识号。

[0067] 硬件处理器203被配置为基于由主人或管理员确定的接入权限和规则来验证从接入信道接收的认证信息。当用户通过接入信道认证时，硬件处理器可以解锁门栓。在本发明的一个方面，当第一冗余接入信道对用户不可用时，硬件处理器203被配置为允许通过第二冗余接入信道接入以解锁门栓。

[0068] 在一些实施例中，智能锁包括用于从和向用户的移动设备收发RFID、NFC或蓝牙信号的无线收发机206。如上所述，用户可以将令牌无线地发送到智能锁104。当无线收发机206接收到令牌时，智能锁如上所述验证该令牌。无线收发机还可以将接入信息传送到用户的移动设备。接入信息提供有关接入事件的详情，例如哪些用户已接入了智能锁以及他们在何时接入。接入信息可以存储在智能锁的存储介质201中。接入信息被存储在智能锁中，直到移动设备接入锁，此时智能锁将把接入信息发送到用户的移动设备。然后移动设备将接入信息传送到中央接入服务器。当用户的移动设备被盗或无法接收无线通信时，智能锁将等待直至下一个有能力的移动设备试图接入智能锁。

[0069] 智能锁锁芯204适合于装入标准规格槽。在本发明的一些实施例中，智能锁的锁芯204是欧规(或“Euro DIN”)设计。在其它实施例中，锁芯可以是椭圆形、圆形、斯堪的纳维亚(Scandinavian)、日本、联合(Union)或Schlage类型的轮廓。然而，欧规锁芯通常在门的内部包括用于接合或脱离门栓的可旋转旋钮，而智能锁具有自由旋转的按钮205。与通常旋转半圈或四分之一圈以接合或脱离门栓的旋钮不同，自由旋转的按钮205可围绕其轴旋转若干次。如下面更详细地解释的，旋转自由旋转的按钮205产生旋转能量，旋转能量可以用于为锁内的电源202通电和再充电几天。

[0070] 当用户的认证信息已被验证时，智能锁被启用以接合门栓。具体地，按钮205可以向内推动，激活与凸轮209接合的离合器。随着用户继续旋转按钮205，凸轮209将门栓从锁定位置移动到解锁位置。用户将无法打开智能锁，直到其被授权进入场地(例如，通过无线发送令牌，提供生物特征扫描或在小键盘上输入密码)。在用户被授权之前，按钮可自由旋转，不会与凸轮啮合。

[0071] 如图2A所示，按钮设置在锁芯的面向外侧的端部。在本发明的一个方面，智能锁使用单个按钮，这使得智能锁适应于不同尺寸或锁规格。例如，自由旋转的按钮205也可以适配于单入口锁、按钮入口锁、双入口锁和挂锁。例如，挂锁可以仅包括自由旋转的按钮而不需要内部旋钮。

[0072] 图2B示出了根据本发明的一些实施例的锁芯的前视图。该按钮可以包括若干接入信道，例如密码小键盘207和生物特征扫描器208，其可以被盖210隐藏。在用户不能使用其移动设备无线发送令牌来解锁门的情况下(例如，用户的移动设备被盗或者设备的电池已经被耗尽)，用户可以通过使用数字小键盘输入密码或者使用生物特征扫描器来获得接入权。

[0073] 如图2C所示，根据本发明的一些实施例，智能锁包括设置在锁芯204的面向内侧的相对端的旋钮或第二按钮211。外部按钮205可以具有比内部按钮211更长的半径和更大的厚度，如下文更详细地解释的，这可以减小旋转按钮所需的力或速度并对其内部电源充电。在智能锁包括内部按钮211的实施例中，内部按钮211可以接合或脱离门栓，而不需要向智能锁提供认证信息或从主人或管理员请求接入。因此，用户可以随时锁定或解锁门以离开场地的内部。

[0074] 图2D示出了在本发明的一些实施例中，按钮可从锁芯拆卸。可拆卸按钮可以包括再充电接口213和输入/输出端口(“I/O端口”)214。电源202可以是可再充电电源，例如电容器组、可充电电池或类似设备。如下面更详细地描述的，按钮还可以包括能量收集元件216。通过从锁芯中移除按钮，用户可以将按钮带到再充电站215，在再充电站215处可以恢复其电荷。再充电站215可以耦合到电源插座，其中电荷可以通过再充电接口213传送到可再充电电源202。再充电接口213可以例如是从具有匹配接口的充电站215接收电流的电线、插头或一个或多个触针。当再充电接口通过匹配的线、插头或触针配置耦合到再充电站215时，再充电站215向按钮供电。可再充电电源202储存从再充电站215接收的电荷。

[0075] 该按钮还可以通过I/O端口214来充电。I/O端口214可以是例如USB、火线(Firewire)、雷电接口(Thunderbolt)、e-SATA、以太网或用于传递电力和/或数据的类似端口。在本发明的一些实施例中，I/O端口214可以从诸如便携式电池充电器的、具有能够输送电荷的匹配接口的外部设备接收电力。例如，外部设备可以是具有USB连接的电池组。在本发明的另外的实施例中，I/O端口214可以从具有匹配端口接口的再充电站215接收电力。再充电站215可以通过I/O端口214将电力从电源插座传递到按钮的电源202。

[0076] 再充电站215可以耦合到主人设备101、管理员设备102或中央接入服务器106。例如，再充电站215可以包括用于建立因特网连接并与主人设备101、管理员设备102或中央接入服务器106通信的以太网端口或WiFi发射机。在连接到I/O端口214时，再充电站215可以获取存储在存储介质201中的数据。如上所述，这样的数据可以包括例如用于验证认证信息、保持诸如接入事件和智能锁使用的日志的接入信息以及标识智能锁的信息和数据。然后，再充电站215可以将从存储介质201获取的数据发送到主人设备101、管理员设备102或中央接入服务器106。因此，在按钮被再充电时，其可以将接入信息传送到其他设备或中央接入服务器。

[0077] 根据本发明的一些实施例，I/O端口可以用于将智能锁连接到无线调制解调器。例如，可以将用于提供对蜂窝网络的接入的USB加密狗、数据卡或类似设备插入到I/O端口中，使得智能锁可以通过蜂窝宽带连接与主人设备、管理员设备或中央接入服务器通信。

[0078] 在本发明的一些实施例中，为了从锁芯释放按钮，需要有效凭证。例如，只有在接收到有效的密码或生物特征扫描时，才可以移除该按钮。这样，当按钮设置在门的外表面上时，该按钮可不被盗贼或不受欢迎的破坏者偷走或移除。在其他实施例中，按钮可以被配置为从锁芯中移除，而不需要提供凭证。例如，当按钮布置在门的内表面上时，面向家的内部，可以随时移除按钮。

[0079] 根据本发明的一些实施例，智能锁包括设置在门的内表面上的按钮和设置在门的外表面上的按钮。在这种构造中，设置在门的内表面上的按钮可以是可移除的和可再充电的，而设置在门的外表面上的按钮既不可拆卸也不可再充电。因此，外部按钮从朝向内部按钮的电源获取电力。以这种方式，可以提供具有抵抗外部篡改的外部按钮的节能双按钮智能锁。

[0080] 如上所述，由移动设备传送的令牌可以包含密码，例如用于单次使用的动态密码。在本发明的一个方面，可以自动地从移动设备产生和传送密码，使得不需要来自用户的交互。具体来说，用户的移动设备可以确定或检测到它在智能锁附近。例如，使用移动设备的基于位置的功能，移动设备可以确定用户正在接近场地。在一些实施例中，可以通过分析过

去的用户模式来帮助确定，并且推断出用户正在从工作回家并且正在其打开他们的家门的路上。移动设备可以替代地通过使用其NFC/蓝牙或无线能力进行该确定。在检测到锁时，移动设备可以识别锁和锁护卫的场地。然后，移动设备可以自动地将该信息传送到中央接入服务器，以确定用户是否被允许接入智能锁。如果用户满足接入锁的所有条件(例如，允许用户在特定时间和日期接入锁)，则接入控制系统将生成动态密码。动态密码可以在主人设备、管理员设备或中央接入服务器处产生，然后被发送到移动设备，或者替代地，其由用户的移动设备上的移动应用产生。然后，移动设备可以将密码发送到智能锁，智能锁使用存储在锁中的进程来验证密码。一旦验证了密码，用户可以向内推动按钮，并使用离合器系统接合或脱离门栓。如果不允许用户打开锁，管理员将接收到未经授权的用户试图打开锁的通知。

[0081] 根据本发明的一些实施例，按钮包括基于操作模式改变颜色的光指示器212。例如，如果认证信息已经被接受，则灯光发绿光；如果验证信息被拒绝，则会发红光；在待机模式下，它会发蓝光。

[0082] 如上所述，智能锁由电源202供电。在本发明的一些实施例中，按钮包括冗余电源，如图3所示。冗余电源可用于在其中一个电源故障的情形下对存储介质、无线收发机和灯光指示器通电。冗余电源可以是例如位于按钮内的一组电容器或电池301。当电池或电容器处于低电荷时，按钮可以将该信息传送到下一个接入锁的移动设备。然后，移动设备可以将该信息传送给主人或管理员。可替代地，可以使用颜色指示器来传送低电荷或电池电量。

[0083] 在其他实施例中，按钮具有通过按钮的旋转运动而被充电的一组电容器301。通过旋转运动储存的能量足以支撑数天，并且如果另一个电源(例如，电池)故障，则提供方便、可靠和冗余的电源。按钮可绕其中心轴自由旋转，产生高水平的动能。而一些旋钮限制为四分之一圈或半圈，按钮可以旋转一整圈。类似于手表上的表冠的上发条，按钮的旋转运动被收集并由按钮内的元件转换成电能，并且储存以供将来使用。按钮旋转越大的转数，锁中储存的电荷就越高。在一个示例性实施例中，按钮的旋转运动驱动一系列齿轮和弹簧302，其传递通过转动按钮产生的旋转能量。由于锁内的弹簧和齿轮302可以小于按钮，所以按钮可以以较低的速度和扭矩旋转。因此，通过针对锁中的齿轮和弹簧按比例地调整按钮的尺寸，可以减小为锁充能的力量。

[0084] 在其他实施例中，按钮的旋转运动被施加到压电元件303。当用户旋转按钮时，按钮的旋转运动被施加到产生压电的压电元件，压电然后被转移并作为电荷储存在电容器组或电池中。压电可由按钮旋转引起的应变、张力或扭转而产生。应变、张力或扭转被施加到压电元件，并产生可以储存在电容器组中的电荷。在其他实施例中，可以通过将旋转运动转换成振动能量来产生压电。具体来说，按钮内部的齿轮或弹簧可与随着按钮的每次转动而振动的压电片接触。

[0085] 在其它实施例中，旋转运动可另外转换成静电能或电磁能。例如，按钮的旋转可以用作使发电机304中的电枢旋转的机械能。在另外的实施例中，按钮的旋转运动可以储存在弹簧或类似的机械装置中。

[0086] 在本发明的一些方面，可以通过收集按钮的旋转运动或通过再充电接口来对按钮进行再充电。以这种方式，如果能量收集部件停止正常工作，再充电接口仍然可用于对按钮再充电，反之亦然。因此，再充电接口和能量收集部件可以以互补的方式操作，以确保按钮

能够被再充电。

[0087] 尽管图2A-D和图3描绘了按钮内部的多个部件，但是在本发明的其它实施例中，这些部件可以放置在按钮的外部。例如，无线收发机、存储器，硬件处理器和电容器/电池组可以设置在锁芯外部，按钮位于锁壳内。这些组件可以通过锁芯与按钮耦合。在其他实施例中，这些部件可以在锁芯内或门接线盒内。

[0088] 图4示出了根据本发明的实施例的使用具有接入信道的锁的过程。在步骤401中，用户选择第一接入信道。如果信道如步骤402所示可用，则用户可以提供认证信息404。例如，如果接入信道将令牌无线地发送到智能锁，则如果例如用户的移动设备丢失、被盗或电量耗尽则可以确定接入信道不可用。如果第一接入信道不可用，则选择第二冗余接入信道403。例如，第二冗余接入信道可以是输入到智能锁的小键盘上的密码或生物特征扫描。

[0089] 如步骤405所示，智能锁验证认证信息。如上所述，如果认证信息包括令牌或密码，则将令牌或密码与存储在智能锁上的进程所产生的令牌或密码进行比较。如果认证信息是生物特征扫描，则将扫描的数据与存储在智能锁中的生物特征数据进行比较。以这种方式，本发明提供冗余的接入信道，其确保即使当用户的移动设备丢失或不可操作时，用户也可以接入锁。

[0090] 如果认证信息被验证，则检查接入权限以确定用户是否被授权接入智能锁，如步骤406所示。例如，确定主人或管理员是否允许用户在给定的日期或时间接入智能锁。如果用户被授权打开锁，则用户被准许接入，并且该按钮可以接合凸轮以打开智能锁407。如果认证信息无效，或者主人或管理员决定拒绝用户接入锁，该按钮将不接合凸轮并打开智能锁408。如上所述，可以在用户设备、中央接入服务器、主人设备或管理员设备处检查规则和接入权限。

[0091] 图5示出了根据本发明的实施例的用于控制具有接入信道的锁的过程。在步骤501中，登记触发事件。触发事件可用于自动启动打开智能锁的过程。触发事件可以是例如当用户的移动设备进入智能锁的预定距离(例如，10英尺)内。然后，触发事件可以例如使得移动设备自动地将令牌发送到按钮。

[0092] 可以基于移动设备的其他能力来登记触发事件。例如，如果移动设备具有手势识别传感器和软件，则可以基于用户何时以特定方式摇动其移动设备来登记触发事件。可替代地，当用户选择按钮或者在移动设备上的移动应用上输入代码时，移动设备可以登记触发事件。

[0093] 在移动设备登记触发事件之后，移动设备识别其正在打开的智能锁，如步骤502所示。然后确定规则是否被配置为准许用户附条件的接入权限或固定接入权限，如步骤503所示。如果用户具有附条件的接入权限，则移动设备将向主人或管理员提交请求，如步骤504所示。否则，在步骤505中评估规则和接入权限以确定用户是否被授权打开锁。

[0094] 如上所述，移动设备可以以多种方式向管理员提交请求。例如，移动设备可以使用其数据连接、通过发送文本消息或者通过向具有呼叫中心的中央接入服务器呼叫来向主人设备、管理员设备或中央服务器提交请求。在本发明的一些实施例中，主人、管理员或中央接入服务器可能要求用户在发出令牌之前提供附加凭证。例如，用户的移动设备提交的请求可以包括用户的位置、口令或其他类似的标识凭证，例如他们的电话号码或电子邮件地址。作为另一示例，附加凭证可以包括证实用户位于智能锁位置的用户的移动设备的GPS坐

标。在其他实施例中，还可能要求用户拍摄智能锁的照片，并向其提供证明用户位于智能锁的位置的请求。凭证成功验证后，会将令牌发送给用户的移动设备。

[0095] 如果主人或管理员批准用户的请求，或者用户具有足以打开锁的接入权限，则用户可以接收令牌，如步骤506所示。如果主人或管理员拒绝了用户的请求，或者用户未经授权打开锁，则用户将不会收到令牌，如步骤507所示。

[0096] 然后，用户可以向智能锁提供认证信息，如步骤508所示。如果用户将通过在小键盘上输入密码来打开锁，则用户可以例如接收作为文本消息或显示在移动应用上的密码，用户可以在智能锁小键盘上输入该密码。如果用户的移动设备无线地将令牌发送到智能锁，则移动设备一旦接收到令牌就可以自动发送令牌。

[0097] 在本发明的一个方面，在认证信息可以提供给智能锁之前，可以需要附加的安全层。例如，在移动设备认证信息无线地发送到按钮之前，可以提示用户在移动设备中输入口令。在其他实施例中，规则可以被配置为要求用户在接收令牌之前在移动设备上扫描其指纹。如上所述，移动设备还可以自动发送认证信息，而无需用户的进一步交互。例如，移动设备可以在启动移动应用时发送认证信息。

[0098] 在一些实施例中，按钮可以是可以从单个接口控制并且基于在接入控制系统中发生的事件而自动化的设备互连集线器的一部分。例如，设备互连网络可以包括通过WiFi或蓝牙无线通信的家用恒温器、照明系统、音响系统和接入控制系统。家用恒温器、照明系统、音响系统和接入控制系统可以使用相同的应用编程接口(“API”)彼此通信或与中央服务器进行通信。使用API，家用恒温器、照明系统、音响系统和接入控制系统可以基于某些规则或事件来自动化。例如，在用户利用他的移动设备解锁他的家门之后，接入控制系统可以将用户偏好传送给恒温器以在一定温度下打开空调器，打开客厅中的某些照明设备，并开始通过扬声器系统播放特定的用户定义的音乐。

[0099] 在本发明的一些实施例中，设备互连集线器根据为用户、管理员或主人定制的设置而进行操作。当人员登记触发事件时，它们被识别，并且设备互连集线器根据对该人员定制的设置进行操作。例如，家长可以配置互连设备集线器的设置，使得当家长解锁前门时，卧室和厨房中的灯被打开，来自特定播放列表的音乐在客厅音响系统上播放，并打开空调/暖气使房屋温度达到70°。孩子可以配置不同的设置，其打开房屋的不同的灯，播放不同的播放列表，并将房间的温度加热/冷却到不同的温度。因此，如果家长解锁家的前门，从而登记触发事件，则设备互连集线器可以根据家长定义的定制设置来操作，并且打开卧室和厨房中的灯，从在客厅音响系统中的特定播放列表播放音乐，并打开空调/暖气以使房屋温度达到70°。

[0100] 在一些实施例中，如上所述的门的移动或位置可以登记引起设备互连集线器执行某些任务或任务序列的触发事件。例如，当确定门被打开时，可以登记触发事件以与恒温器通信以在一定温度下打开空调器，打开客厅中的某些照明设备，并开始通过扬声器系统播放特定用户定义的音乐。

[0101] 图6示出了使主人或管理员能够控制接入控制系统的过程。在步骤601中，向主人或管理员显示一组可配置的规则和接入权限。在步骤602中，主人或管理员配置接入权限以确定用户可以接入哪些智能锁。在步骤603中，主人或管理员配置指定用户可以使用哪些接入信道来打开智能锁，以及在打开智能锁之前必须满足何种(如果有的话)条件的规则。

[0102] 当具有附条件的接入权限的用户如上所述提交打开智能锁的请求时，主人或管理员接收接入请求，如步骤604所示。例如，可以以文本消息、电话呼叫或作为显示在主人或管理员的移动应用上的通知的形式接收请求。该请求可以直接从用户接收，或者可以从接收到来自用户的请求的中央接入服务器接收。

[0103] 在步骤605中，用户请求被验证。可以通过例如要求用户提供诸如口令的附加凭证来验证用户。作为另一示例，主人或管理员可以获得用户的移动设备的ID以确定移动设备是否已被报告为丢失或被盗。如果被盗，则可以将规则配置为自动拒绝接入请求，并将尝试使用通知主人、管理员或用户。

[0104] 如果主人或管理员验证用户，则主人或管理员可以进行到步骤606，其中主人或管理员确定是否准许用户接入。在此步骤中，可以检查规则和接入权限以确定用户是否被授权打开特定的锁，并且在打开锁之前是否必须满足任何条件。例如，可以确定用户没有被授权打开特定智能锁，或者没有被授权在特定的一天打开智能锁。如果用户被授权，主人或管理员可能仍然决定拒绝用户接入。例如，即使用户被授权，主人或管理员也可能更愿意使用自己的判断来批准请求。如果主人或管理员确定批准请求，则生成令牌或密码并将其提供给用户。令牌或密码可以如上所述发送给用户。例如，令牌或密码可以以文本消息、电话呼叫或作为在用户的移动应用上显示的通知的形式发送。然后可以在步骤608将令牌或密码提供给用户。

[0105] 根据本发明的一些实施例，可以在主人设备、管理员设备或用户设备上安装移动应用，用于控制使用接入控制系统。主人或管理员的移动应用可以提供以下接口：查看接入信息；创建接入权限；查看接入日志；管理用户权限；打开锁；以及创建成功进入以及拒绝进入的报告，包括为什么进入被拒绝的详情(例如，用户在允许其接入锁的时间表或日期之外接入锁，或者起初就不允许用户打开锁)。以这种方式，接入控制系统提供了机械锁和钥匙系统的安全和可靠性优势，同时还提供了移动设备和电子锁系统的报告和实时增值服务。类似地，用户的移动应用可以提供以下接口：接收接入警报；请求接入权限；查看接入日志；以及打开锁。

[0106] 在本发明的一个方面，移动应用提供如图7A所示的“通知者”特征，其向主人、管理员和用户通知有关接入事件和接入权限的信息。对于主人和管理员，移动应用将接收有关接入事件的信息，例如用户何时接入锁。如图7A所示，该特征向主人或管理员提供了约翰逊史密斯希望打开大门，靠近大门，或正试图打开大门的警报。该警报近实时地将接入事件或接入权限的变化通知主人或管理员。由于可以将事件快速传送给主人或管理员，因此移动应用可以另外近实时地向主人或管理员提供拒绝用户接入受保护场地的选项。类似地，当用户尝试用无效认证信息(例如，不正确的密码)打开锁时，移动应用也可以接收警报。

[0107] 使用移动设备的无线或基于位置的能力，移动应用可以确定用户停留在受保护场地的时间长度。移动应用还可以从按钮接收关于其何时被锁定和解锁的信息，以确定用户何时获得接入并随后离开受保护场地。如下面更详细的解释，锁上的按钮也将其锁定/解锁状态发送给用户的移动设备。然后，用户的移动设备可以向中央接入服务器发送锁定/解锁状态，然后中央接入服务器可以向主人或管理员发送关于锁状态的通知。以这种方式，在用户随后离开受保护场地之后，主人或管理员可能会被告警该场地仍然被解锁，并且可以联系用户通知其忘记锁定场地。

[0108] 在本发明的一个方面，移动应用可以向主人或管理员显示已经锁定或解锁受保护地点的哪些区域，如图7B所示。当用户使用其移动设备解锁或锁定场地时，移动设备将信息传送到中央接入服务器。然后，中央接入服务器向主人或管理员提供锁定/解锁状态。当用户使用替代的接入信道来锁定或解锁场地时，该信息被存储在智能锁上，并且在下一次使用移动设备来打开智能锁时被传送到中央接入服务器。

[0109] 移动应用还被编程为提供用于显示和配置这些场地如何被解锁的用户接口。例如，如图7C所示，移动应用可以显示场地是否可以自动或手动打开。

[0110] 移动应用的另一个接口提供哪些用户可以接入锁的显示。如图7D所示，接口显示每个用户的图片及其个人信息，如姓名和联系信息。可以选择或删除列表中的每个用户。选择用户会导致移动应用显示另一个显示有关用户的附加详细信息的接口。

[0111] 在本发明的一个方面，通知者将显示关于对用户的接入权限所做的改变的警报和消息。如图7E所示，通知者可以告知用户其在特定时间(例如从星期一到星期五，从下午5点到下午8点)对特定场地(例如，大门A)具有接入权限。类似地，通知者可以通知用户其接收到对特定区域的新的接入权限，或者这些接入权限已被限制或被撤销。

[0112] 虽然图7A-7E示出了使用移动应用接口的通知者的警报和消息传递功能，但是关于接入权限的警报和消息也可以通过SMS文本、电子邮件或通过电话传送给用户。因此，例如，当用户接入权限改变时，用户可以接收通知用户其接入权限已被改变的SMS文本。

[0113] 在本发明的一个方面，移动应用提供了一个“授权”功能，其使得主人和管理员能够创建和改变用户的接入权限，并允许用户请求接入权限。每个用户的接入权限存储在主人设备、管理员设备或中央接入服务器中，其中可以对每个用户接入锁的尝试进行验证。

[0114] 如图8A所示，移动应用可以为主人或管理员提供用于创建用户接入权限和规则的接口。例如，该接口允许主人或管理员指定用户的联系信息(例如，姓名，电话号码，职业，年龄)，用户将具有接入权限的特定个人锁，用户可以使用的接入信道(例如，密码，生物特征扫描，将令牌无线发送到智能锁，或其任何组合)，以及对用户接入的条件(例如，对一天中的时间的限制)。移动应用的授权功能可供主人和管理员使用。在管理员使用的授权特征的一些实施例中，在提供接入信息之后，管理员将该信息作为请求提交给主人。然后将信息传送给最终批准或拒绝为新用户创建接入权限的主人。接入权限的创建可能近实时地发生；当主人批准用户的请求或管理员的请求时，用户可以立即开始使用他们的移动设备、密码或生物特征扫描来接入指定的智能锁。

[0115] 在本发明的一个方面，主人或管理员可以指定场地内的特定的锁、区域或门，如图8B所示。如图8B所示，主人或管理员可以选择诸如前大门、健身房、娱乐室或办公室之类的锁定区域来授权对用户的接入。移动应用可以使得该配置远程且近实时地发生；不需要主人或管理员在现场进行密钥拷贝或更新任何记录而导致延迟。

[0116] 状态可以对应于从上述传感器接收到的对应于门被打开或关闭以及门栓被锁定或解锁的信息。

[0117] 如上所述，授权特征允许主人或管理员添加对用户接入的限制。如图8C所示，主人或管理员可以允许用户具有永久无期限的接入，或者可以限制用户的接入是临时的，或者可以限制接入在一整天，一整周，一整月或一整年中的选定间隔期间内。

[0118] 授权特征还可以允许主人或管理员根据具体情况提供一次性接入。如上所述，用

户可以通过向主人或管理员发送请求来接收一次性接入。该请求可以通过移动应用的用户授权接口、SMS文本、电子邮件或通过电话呼叫。该请求可以针对特定的锁或锁组，以及针对特定的接入类型。主人或管理员可以近实时地确定准许或拒绝该请求。如果主人或管理员批准请求，则用户可以打开锁。使用记录和报告功能，主人或管理员可以确定用户何时完成使用锁，并禁用或去除用户的接入权限。可替代地，如果主人或管理员决定准许用户接入，则主人或管理员可以向用户提供只能使用一次的动态密码，并且在使用之后到期。

[0119] 如图8D所示，接入类型接口允许主人或管理员配置规则以指定什么接入信道可用于用户打开智能锁。例如，主人或管理员可以指定用户是否可以通过将令牌无线地发送到智能锁、在小键盘上输入密码、使用生物特征扫描或其任何组合来打开智能锁。主人或管理员还可以添加限制用户何时可以接入智能锁的条件，例如添加时间或日期限制。例如，主人或管理员可以指定用户可以在星期一至星期五使用智能手机或移动设备接入锁，但周末必须另外提供生物特征扫描或密码。

[0120] 在本发明的一个实施例中，主人或管理员可以使用其各自的移动设备将用户的生物特征扫描添加到智能锁。例如，用户可以在智能手机上扫描其指纹，并通过SMS文本或移动应用将其发送给主人或管理员。然后，主人或管理员可以将指纹添加到中央接入服务器，或者在下一次其移动设备与智能锁通信时添加到智能锁中。以这种方式，可以将新用户的生物特征扫描远程添加到智能锁中，而无需用户先前位于智能锁处。

[0121] 用户可以使用其移动设备上的移动应用发送对于接入权限的请求。登记后，用户可以加载场地列表及其相应的锁，并从智能锁的相应主人或管理员请求接入。用户可以搜索主人或管理员，并直接从他们请求接入权限。作为使用移动应用的替代方案，用户可以通过SMS文本、电子邮件或通过电话请求接入。

[0122] 主人或管理员可以在任何时候通过授权接口修改每个用户的接入权限，如图8E所示。在本发明的一个方面，可以修改接入权限，而不通知或告知用户。以这种方式，主人或管理员可以远程地更改或删除与移动设备相关联的接入权限，而不需要与用户的任何接入或交互。因此，如果移动设备被盗或丢失，则主人或管理员可以禁用该特定的移动设备，防止其被未经授权的人员使用或以不期望的方式使用。在移动设备可能被禁用之前，主人或管理员可能会被提示以其他凭据来验证其身份。如果被禁用的手机之后被用于接入智能锁(例如，由盗贼或不期望的人员)，则智能锁将拒绝它，并且主人或管理员将被通知未经授权的接入尝试。如下面的示例性说明所示，授权接口允许主人或管理员取消授权用户，禁用用户或将其从锁中完全移除。对用户接入权限的这些更改可以近实时地实现。

[0123] 在本发明的一个方面，移动应用提供“报告”特征，其使得主人和管理员能够查看每个用户或每个锁的接入事件的记录和日志。诸如用户何时以及如何寻求或获得对智能锁的接入的各种接入事件的记录可以如上所述存储在按钮的存储介质中或存储在用户的移动设备的移动应用中。例如，当用户使用其移动设备寻求或获得对智能锁的接入时，该接入事件的记录可以被存储在移动设备或按钮中。类似地，如果用户经由冗余接入信道(例如，密码或生物特征扫描)来接入智能锁，则接入事件可以存储在按钮中，并且在另一个移动设备与智能锁接触的稍后阶段将无线地传送到中央接入服务器。

[0124] 接入事件还可以包括由上述传感器接收的指示门是否已被打开或关闭或者门栓是否已被锁定或解锁的信息。

[0125] 每个用户或每个智能锁的接入事件的日志可以被周期性地汇编并传送或近实时地传送给主人或管理员。例如，如图8F所示，可以将用户当天的接入事件的日志汇编并报告给主人或管理员。日志显示特定用户的每个接入事件的详情，例如接入了什么智能锁，如何接入该智能锁，以及用户接入它的精确时间，以及用户在场地花费了多长时间。日志可以进一步包括智能锁的成功和不成功打开的记录，允许用户打开智能锁的时间段，以及用户何时请求接入智能锁。可以对于每个智能锁汇编类似的日志，报告谁接入智能锁，如何接入智能锁以及何时接入智能锁。主人和管理员可以配置其比较喜欢收到日志报告的频率。报告可以传送到中央接入服务器，或直接传送给主人或管理员。

[0126] 在本发明的其他实施例中，日志可以直接从智能锁直接传送到管理员或中央服务器，绕过移动设备。如上所述，智能锁可以使用其无线连接或通过网络设备将该信息直接传送到中央服务器或管理员。

[0127] 在本发明的一个方面，可以处理日志和报告以发现关于接入使用和用户的模式。具体来说，可以挖掘日志和报告以检测与用户接入不同智能锁的方式和时间有关的模式。使用这些识别的接入行为模式，接入控制系统然后可以预测接入事件以增强系统安全性或接入控制。例如，如果日志和报告指示用户每个工作日在下午5:00从前大门进入家中，则接入控制系统可以使互连设备中的进程或任务自动化，例如与照明系统通信以激活在前庭院的灯光，恒温器启动空调器。

[0128] 图9A-9C示出了用于登录移动应用，请求令牌或密码以及接收令牌或密码的用户接口。如上所述，可能要求用户在被允许请求令牌或密码之前提供诸如口令的如图9A所示的凭证。如图9B所示，接口允许用户查看他们可以接入的智能锁，以及如果他们没有智能锁接入权限，或者仅具有附条件的接入权限，他们可以向主人或管理员提交请求。如图9B所示，用户可以通过几种方式提交请求，例如通过向主人或管理员的移动设备上的移动应用发送警报，或通过向他们发送文本或打电话。如图9C所示，如果用户已被验证并被主人或管理员批准接入，则用户将接收令牌或密码。如果用户收到密码，则可以显示他们的密码供用户输入到小键盘。如果用户接收到令牌，则令牌可以被无线地发送到智能锁。

[0129] 在本发明的另外的方面，用日志发现的用户模式可以用于优化智能锁的某些组件。例如，日志可以用于确定用户何时通常离开家以及到达家。利用该信息，智能锁可以确定智能锁最不可能使用的某些时间段，并且因此可能改变其功能或其操作模式中的一些。例如，智能锁可以确定在工作日的营业时间内通常没有人进入家或离开家。在此期间，智能锁可能进入“睡眠”模式，其中智能锁会停用某些特征以降低其功耗。

[0130] 在不脱离本发明及其权利要求的精神和范围的情况下，本领域普通技术人员可以想到本文所描述的内容的变型、修改和其他实现方式。

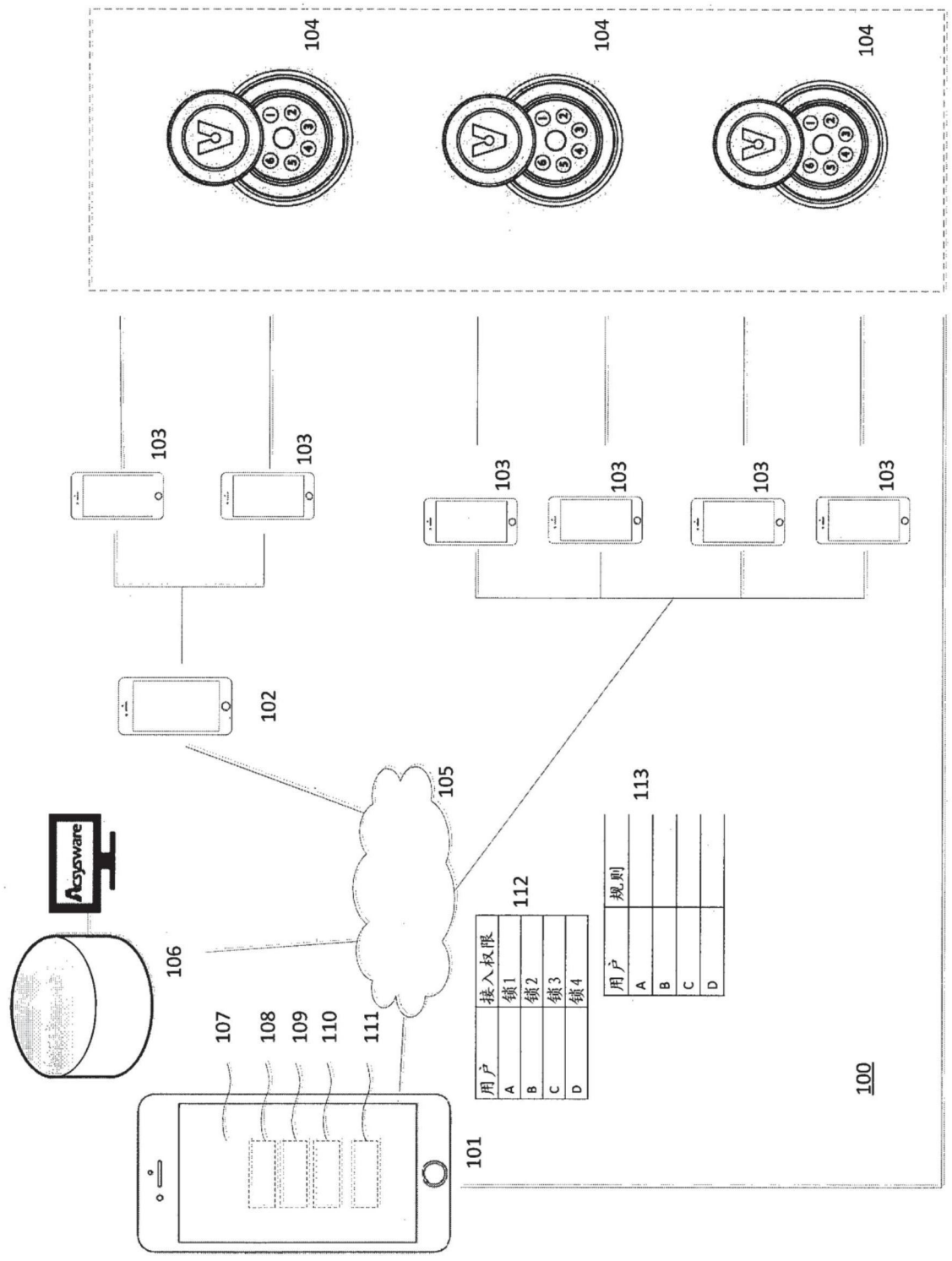

104
104
104
103
103
103
103
103
103
102
105
113
112
106
107
108
109
110
111
101
100
Acsysware
用户
规则
A
B
C
D
用户
接入权限
A
锁1
B
锁2
C
锁3
D
锁4

图1A

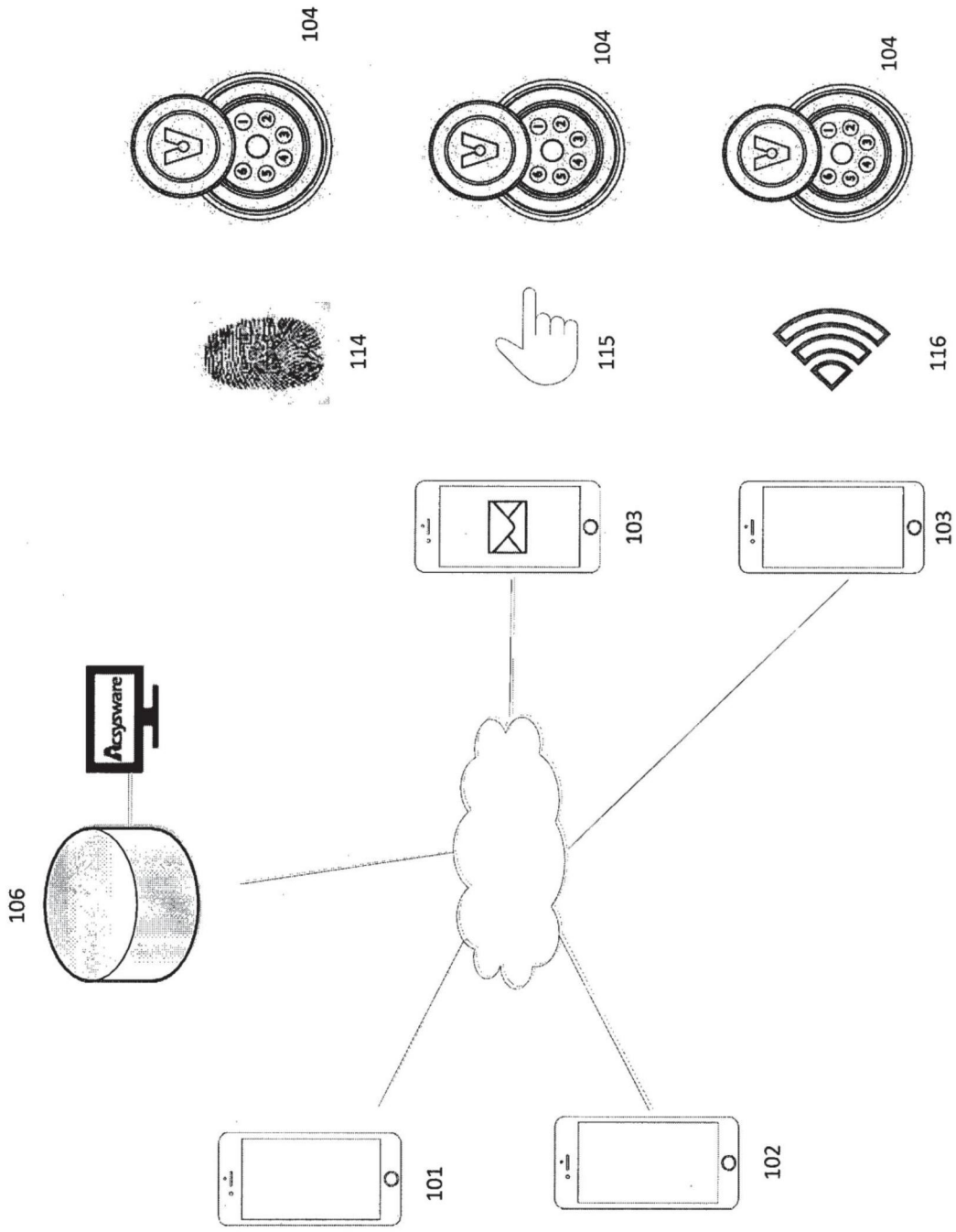


图1B

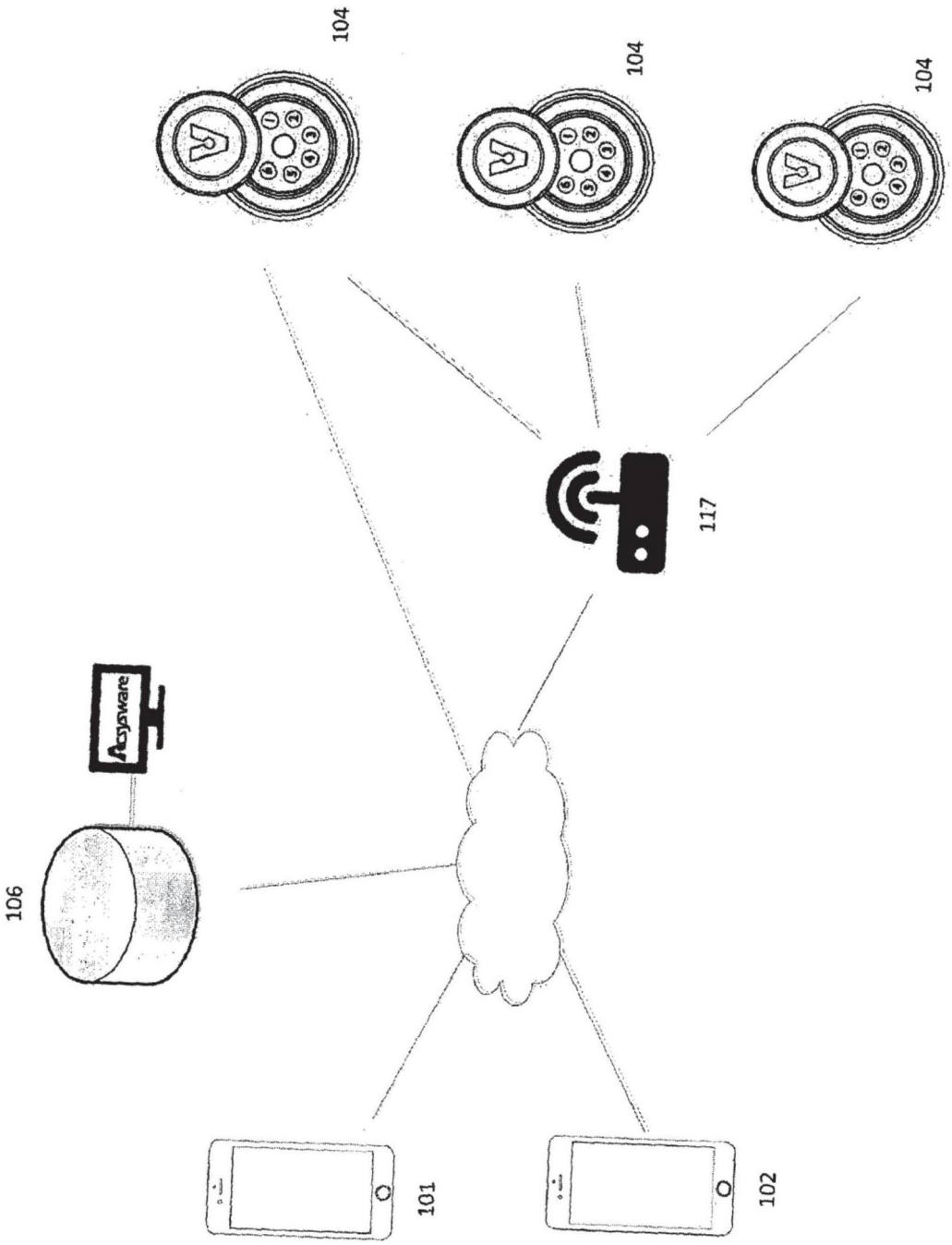


图1C

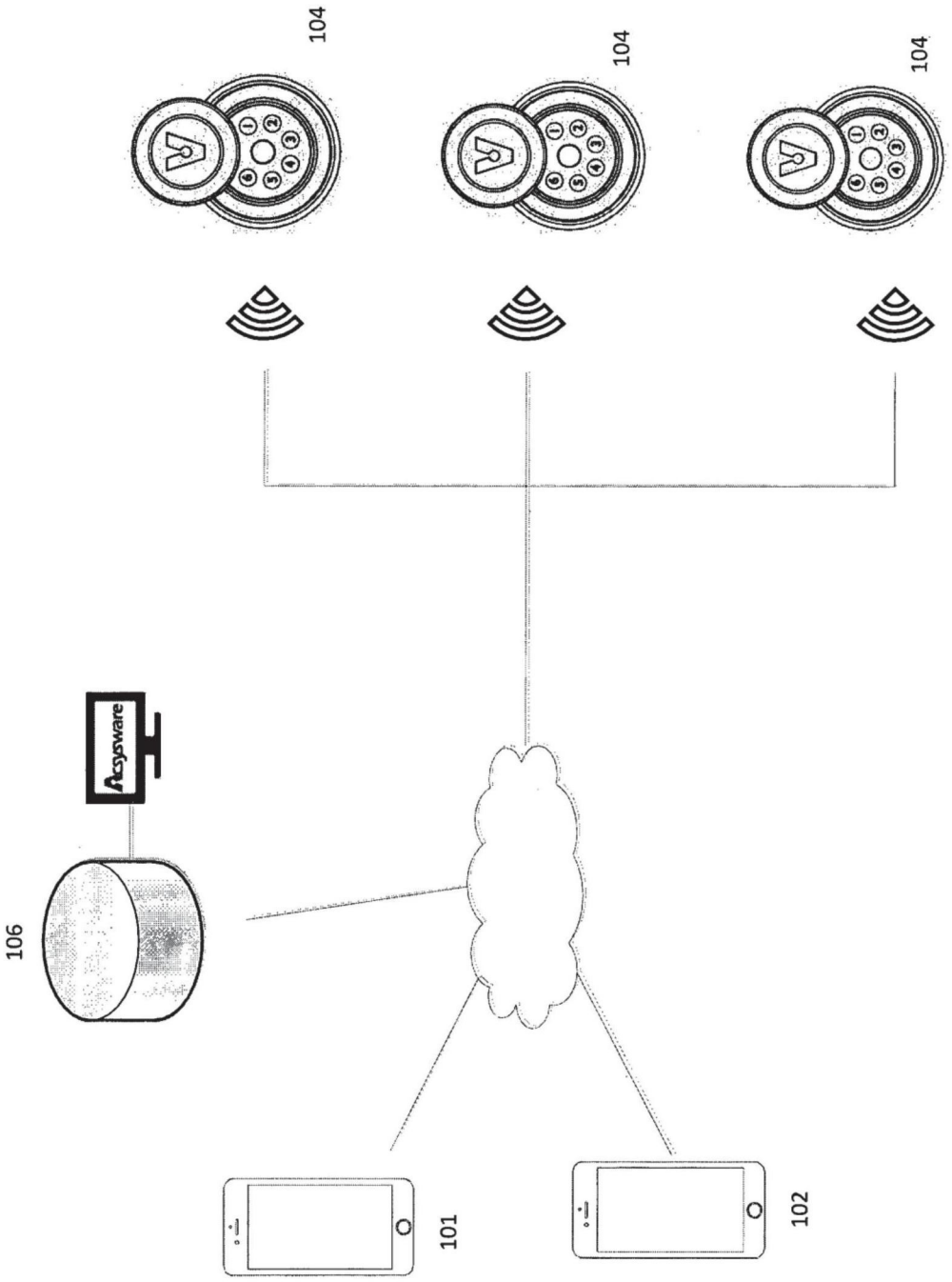


图1D

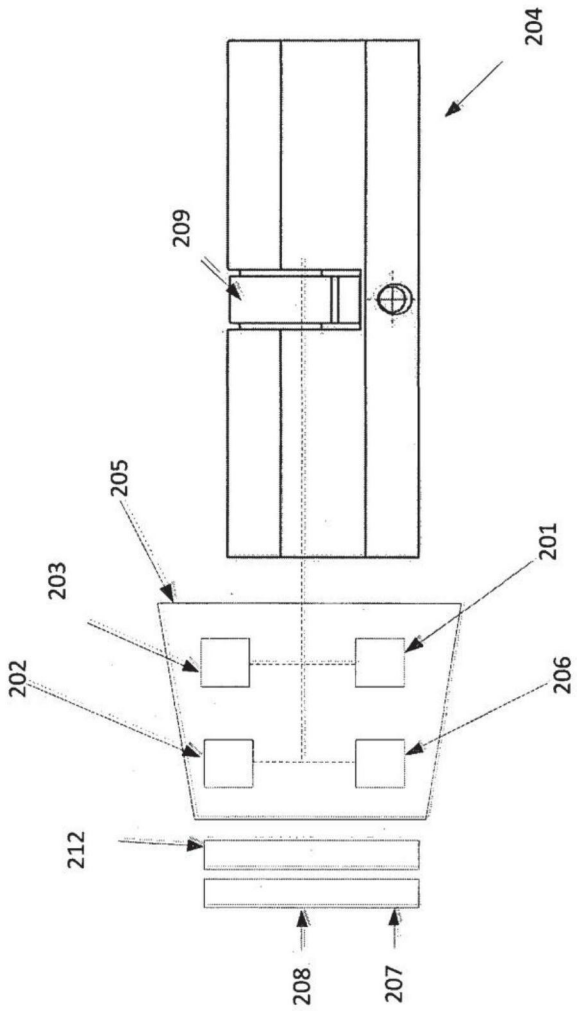


图2A

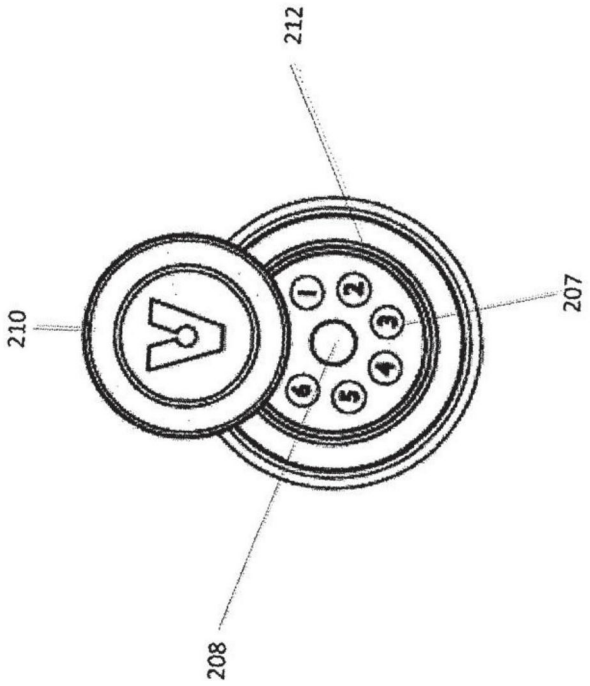


图2B

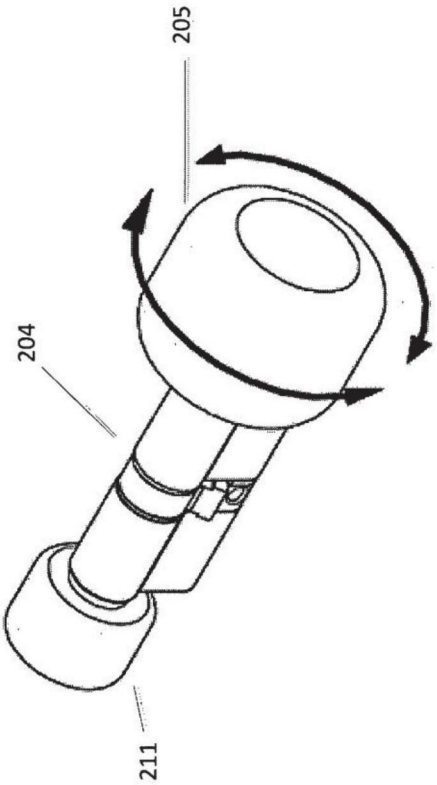


图2C

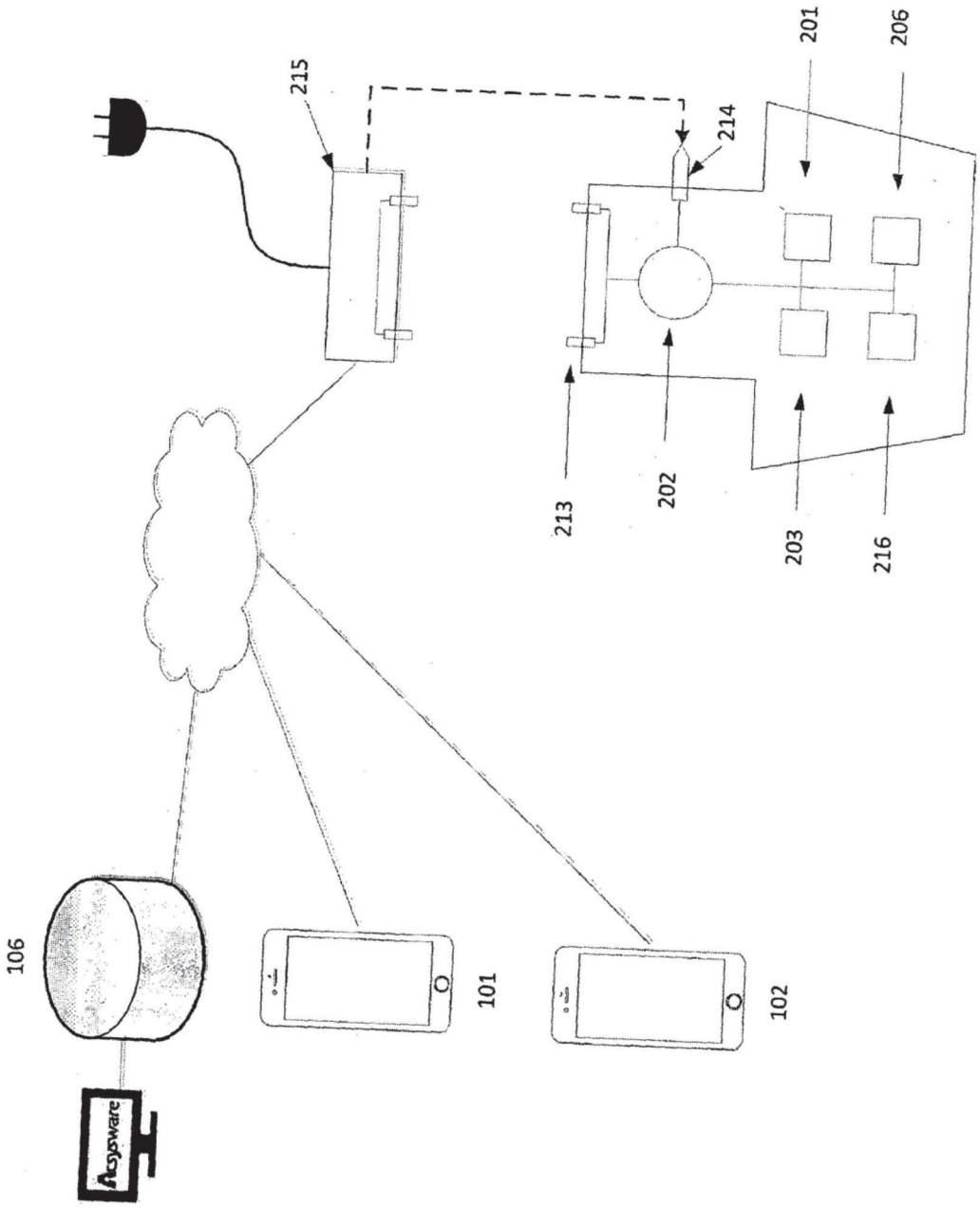


图2D

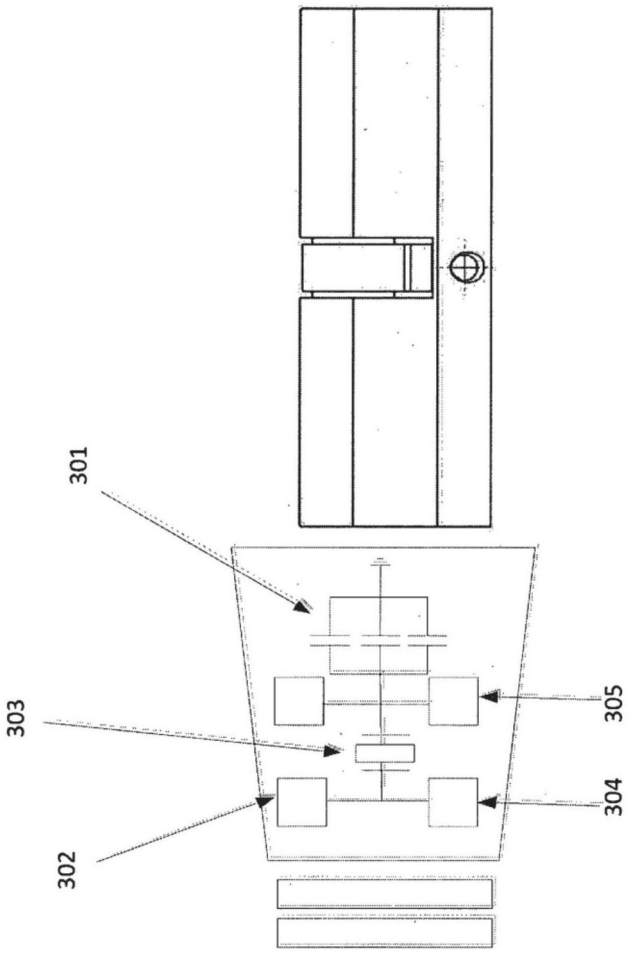


图3

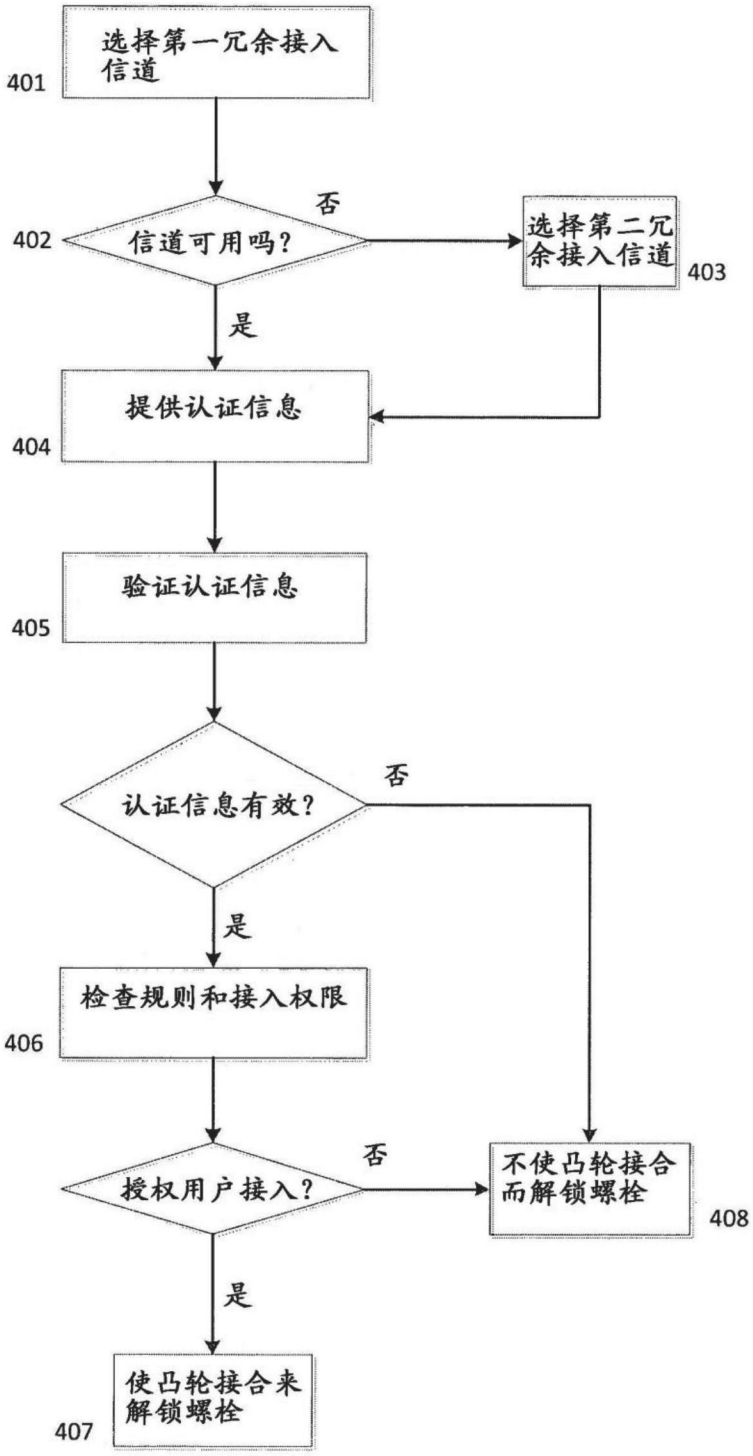

选择第一冗余接入信道
401
信道可用吗?
402
否
选择第二冗余接入信道
403
是
提供认证信息
404
验证认证信息
405
认证信息有效?
否
是
检查规则和接入权限
406
授权用户接入?
否
不使凸轮接合而解锁螺栓
408
是
使凸轮接合来解锁螺栓
407

图4

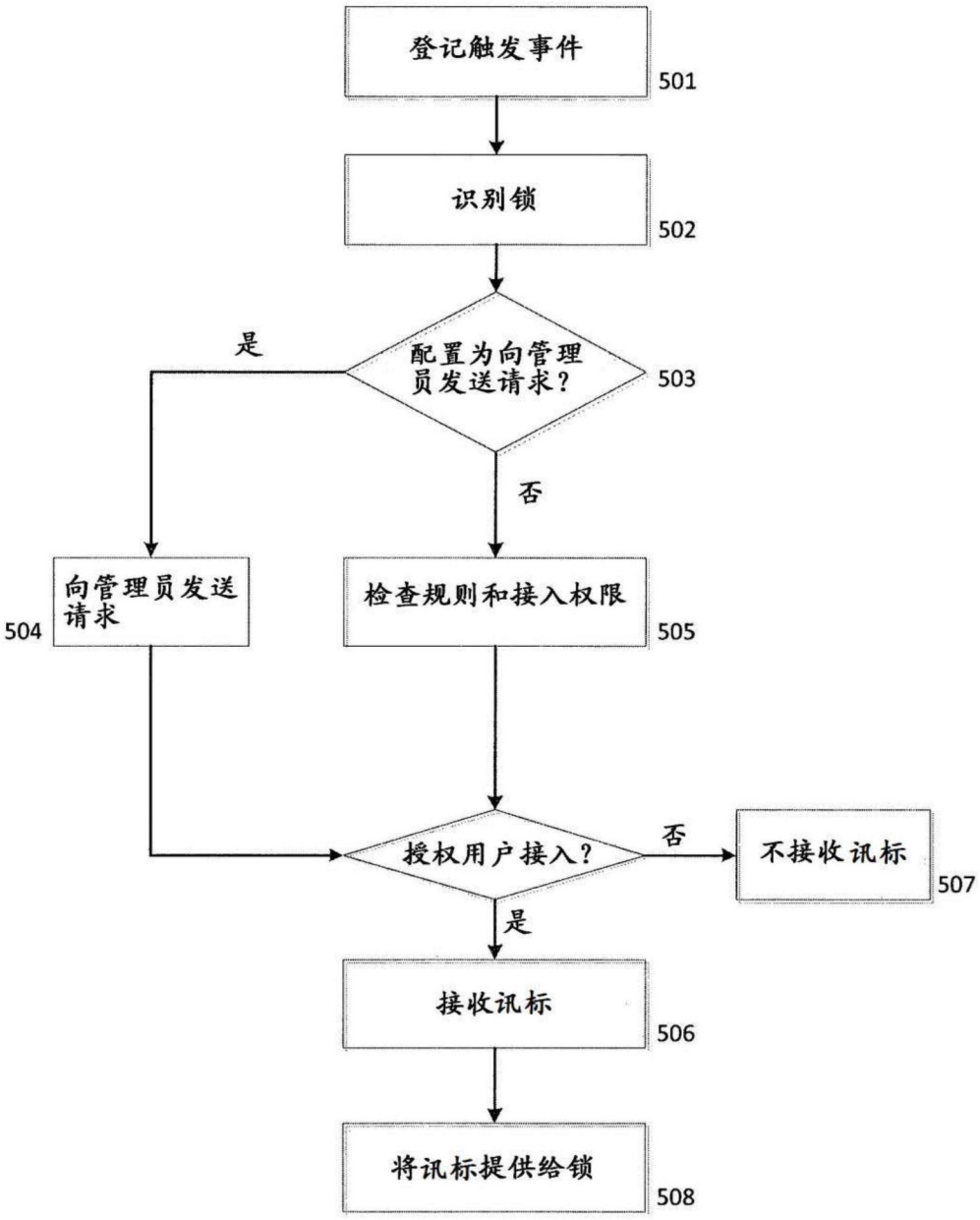

登记触发事件
501
识别锁
502
配置为向管理员发送请求?
503
是
否
向管理员发送请求
504
检查规则和接入权限
505
授权用户接入?
否
不接收讯标
507
是
接收讯标
506
将讯标提供给锁
508

图5

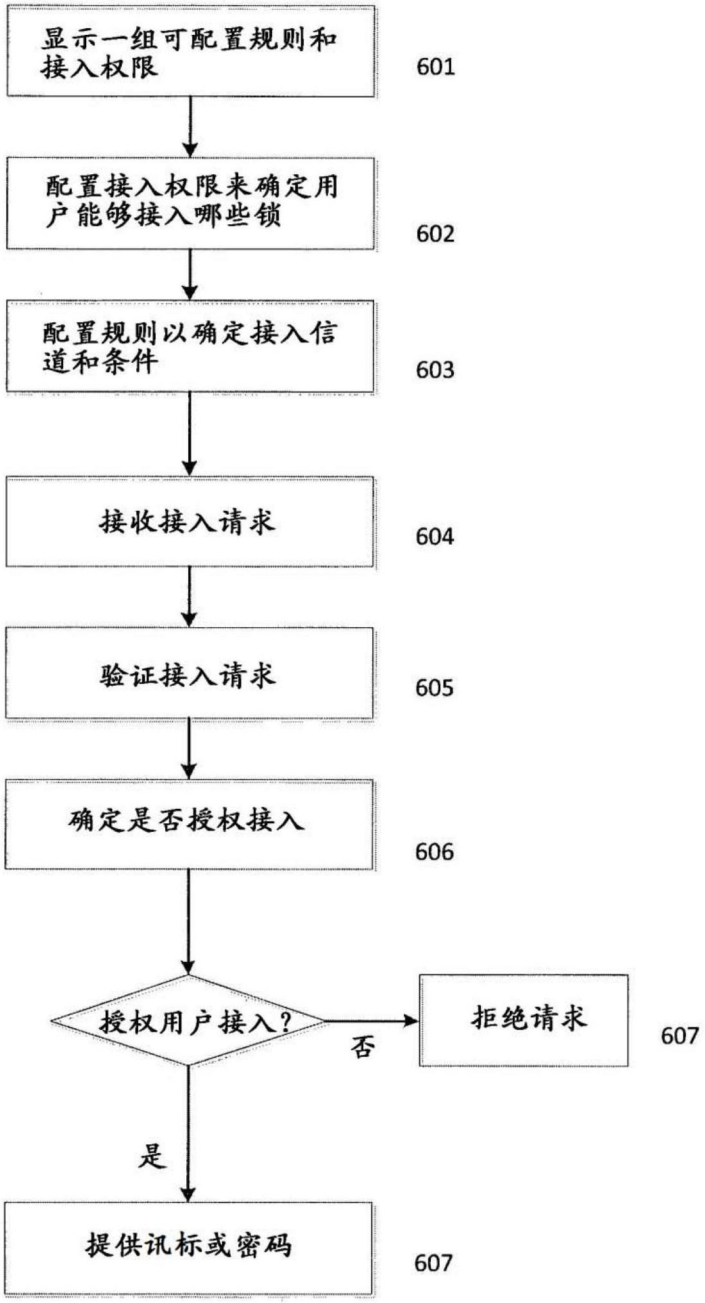

显示一组可配置规则和接入权限
601
配置接入权限来确定用户能够接入哪些锁
602
配置规则以确定接入信道和条件
603
接收接入请求
604
验证接入请求
605
确定是否授权接入
606
授权用户接入?
否
拒绝请求
607
是
提供讯标或密码
607

图6

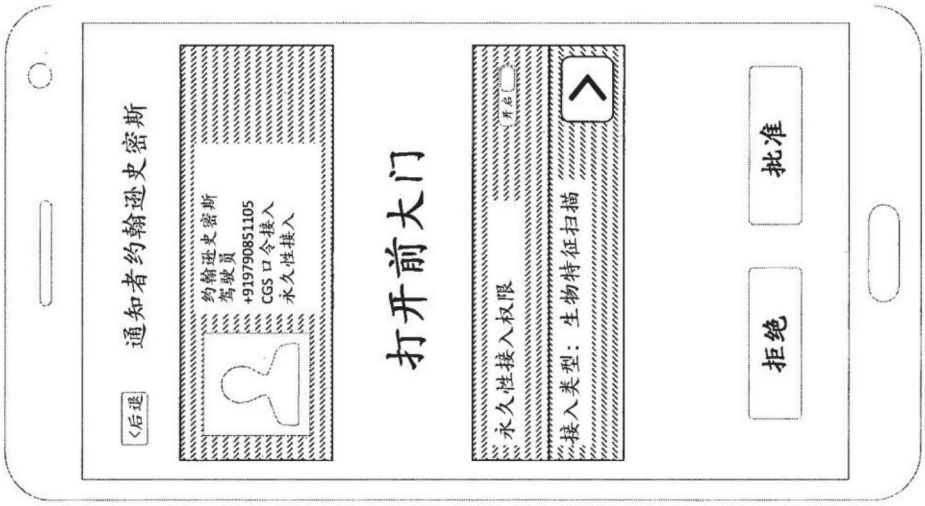

通知者约翰逊史密斯
约翰逊史密斯
驾驶员
+919790851105
CGS 口令接入
永久性接入
打开前大门
永久性接入权限
接入类型：生物特征扫描
拒绝
批准

图7A

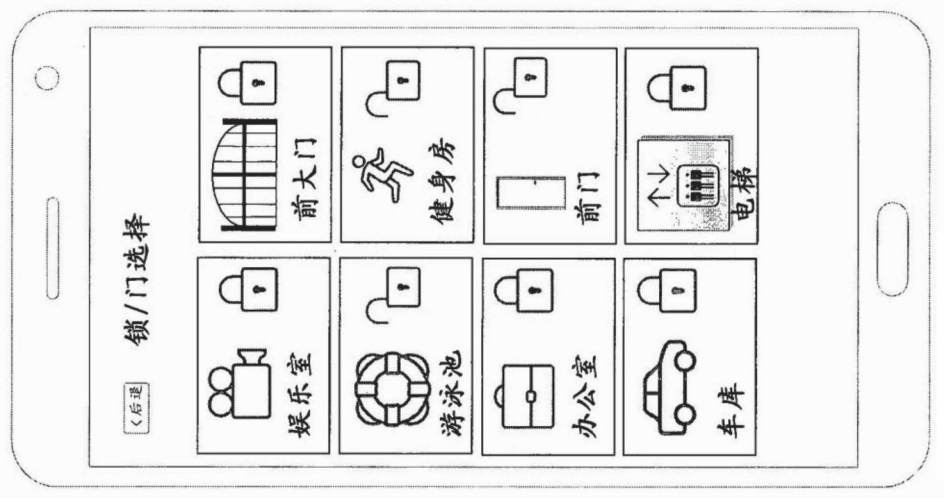

锁/门选择
娱乐室
前大门
游泳池
健身房
办公室
前门
车库
电梯

图7B

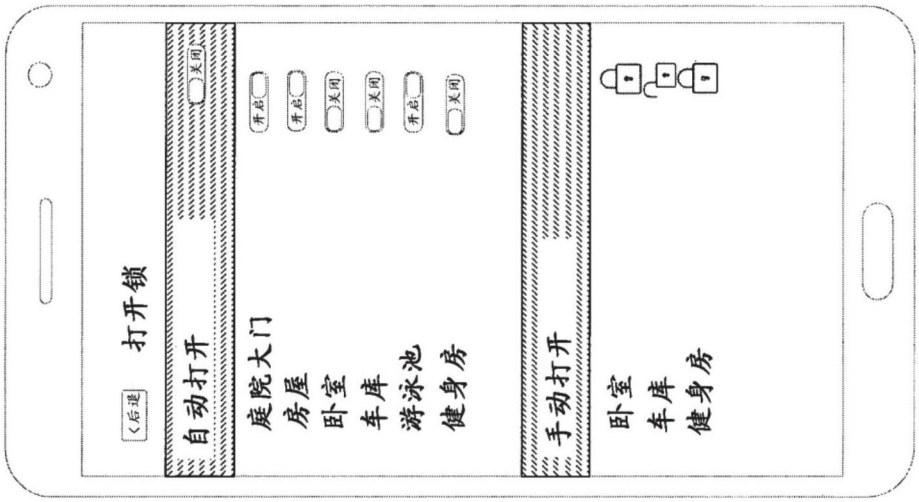

打开锁
后退
自动打开
关闭
庭院大门
房屋
卧室
车库
游泳池
健身房
开启
关闭
手动打开
卧室
车库
健身房

图7C

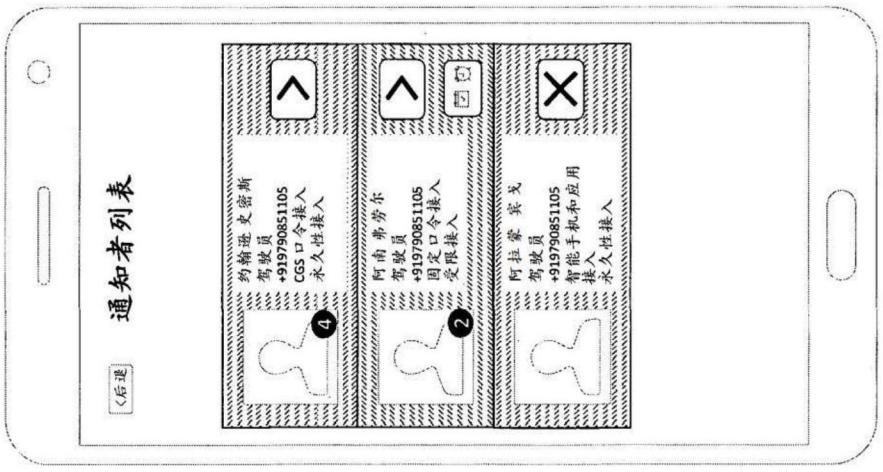

通知者列表
后退
约翰逊 史密斯
驾驶员
+919790851105
CGS 口令接入
永久性接入
4
阿南 弗劳尔
驾驶员
+919790851105
固定口令接入
受限接入
2
阿拉蒙 索戈
驾驶员
+919790851105
智能手机和应用
接入
永久性接入

图7D

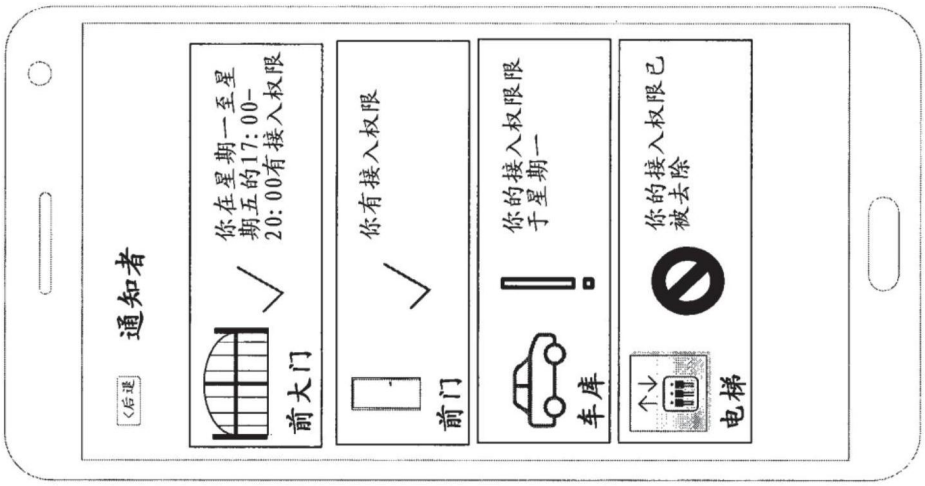

通知者
你在星期一至星期五的17:00-20:00有接入权限
前大门
你有接入权限
前门
你的接入权限限于星期一
车库
你的接入权限已被去除
电梯

图7E

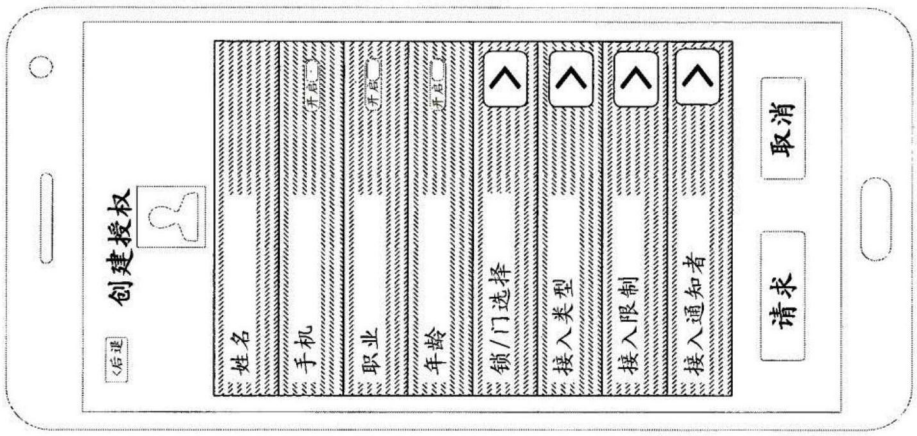

创建授权
姓名
手机
职业
年龄
锁/门选择
接入类型
接入限制
接入通知者
请求
取消

图8A

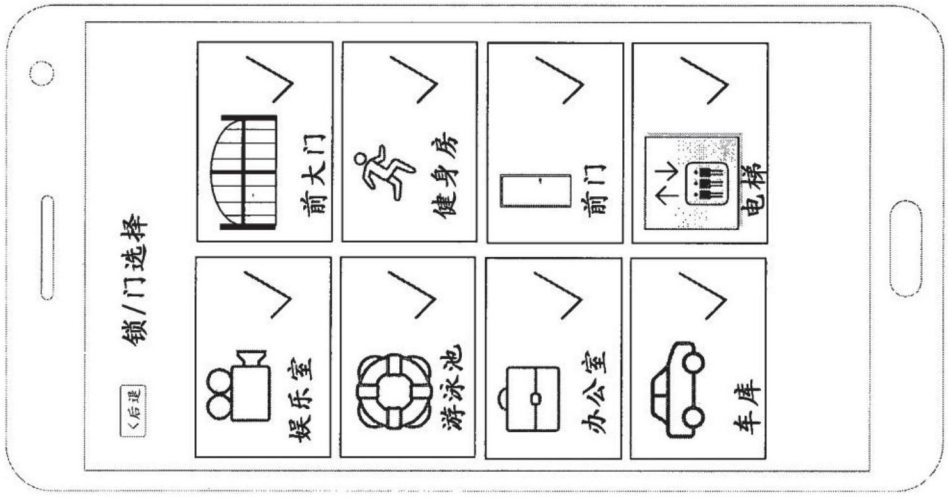

锁/门选择
前大门
健身房
前门
电梯
娱乐室
游泳池
办公室
车库

图8B

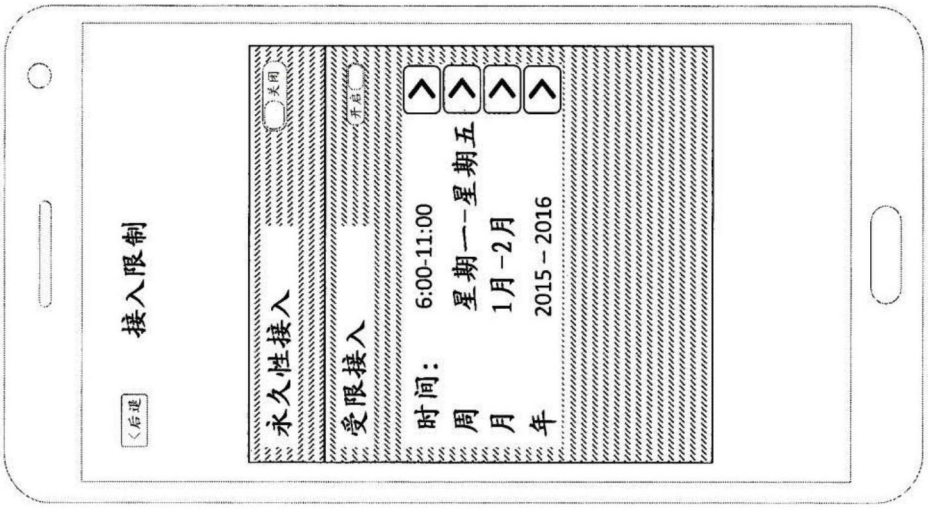

接入限制
永久性接入
受限接入
时间: 6:00-11:00
周 星期一-星期五
月 1月-2月
年 2015-2016

图8C

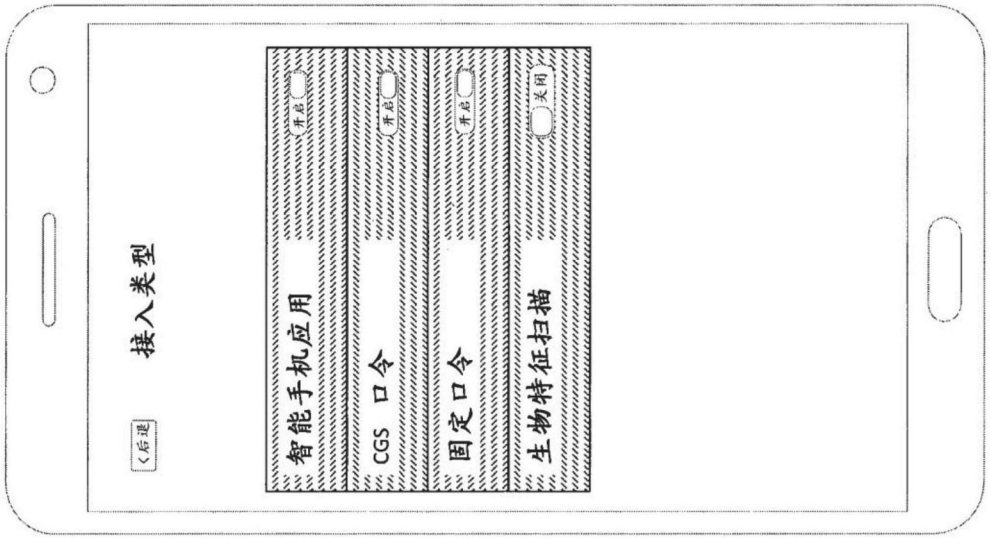

接入类型
<后退
智能手机应用
CGS 口令
固定口令
生物特征扫描
开启
开启
开启
关闭

图8D

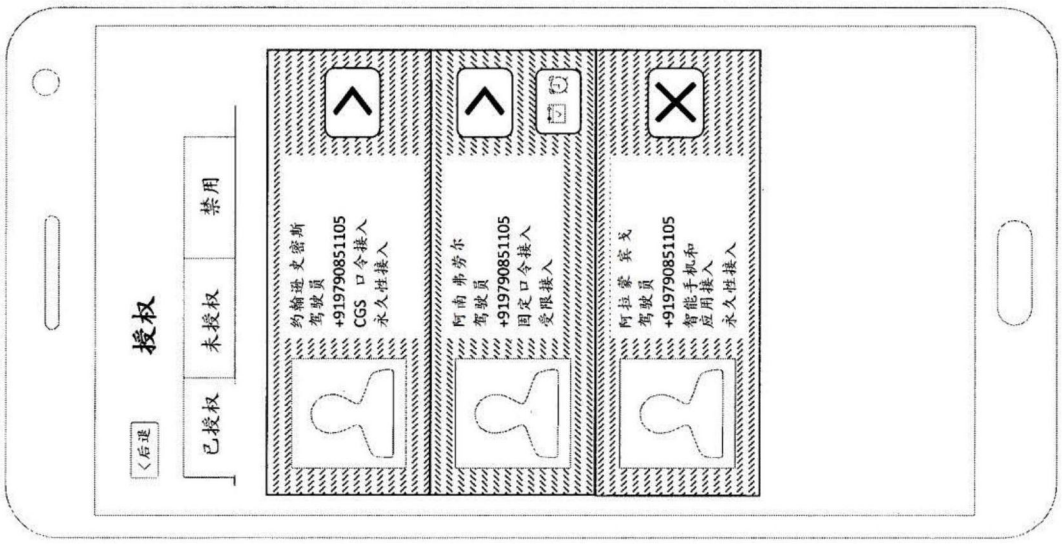

授权
<后退
已授权
未授权
禁用
约翰逊 史密斯
驾驶员
+919790851105
CGS 口令接入
永久性接入
阿南 弗劳尔
驾驶员
+919790851105
固定口令接入
受限接入
阿拉蒙 索戈
驾驶员
+919790851105
智能手机和
应用接入
永久性接入

图8E

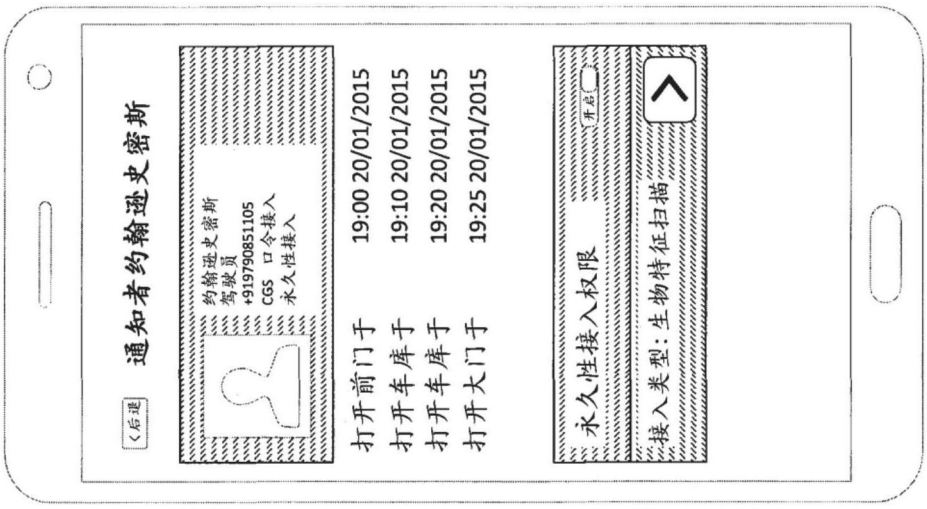

通知者约翰逊史密斯
约翰逊史密斯
驾驶员
+919790851105
CGS 口令接入
永久性接入
打开前门于 19:00 20/01/2015
打开车库于 19:10 20/01/2015
打开车库于 19:20 20/01/2015
打开大门于 19:25 20/01/2015
永久性接入权限
接入类型：生物特征扫描

图8F

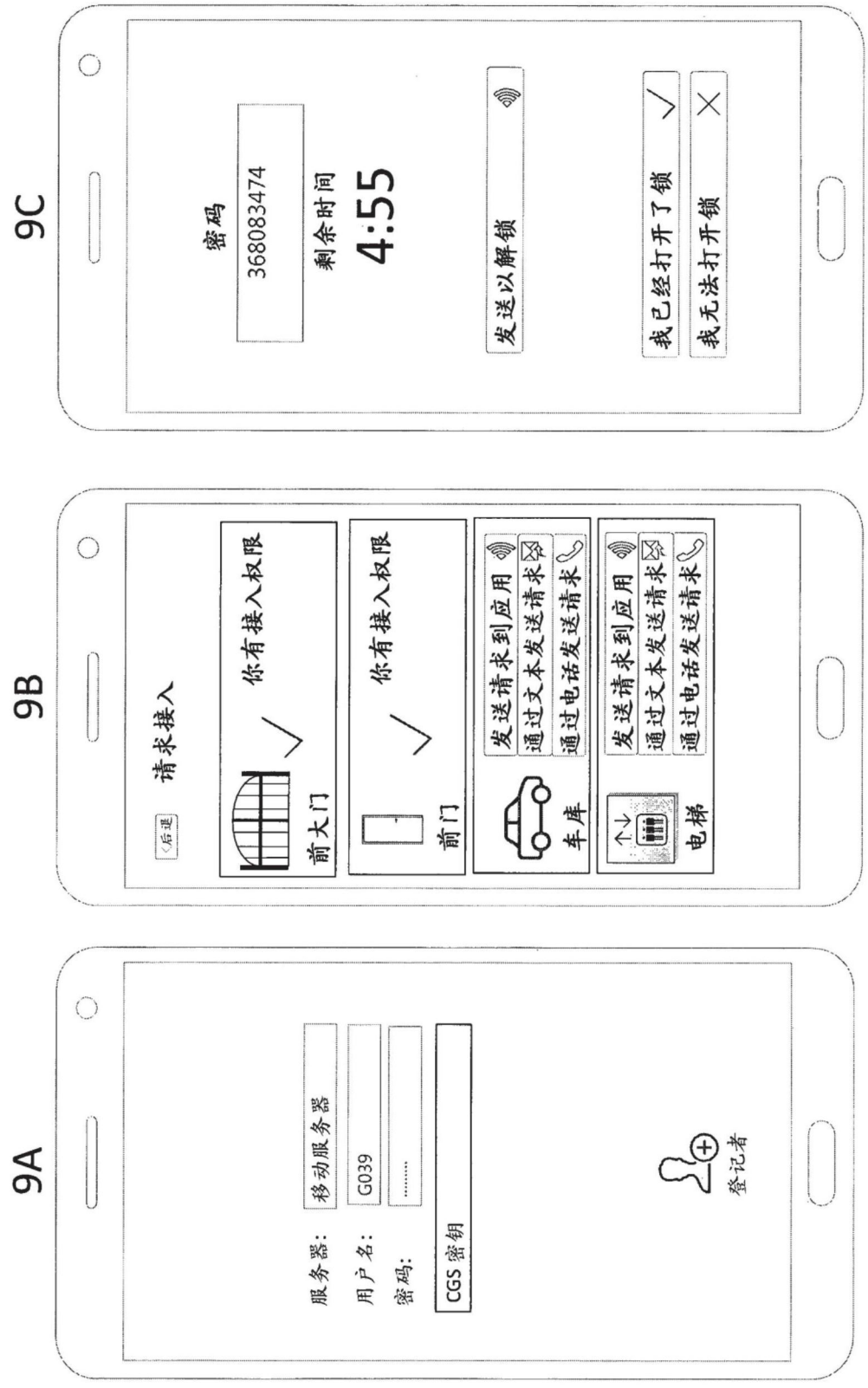

9A
服务器：
移动服务器
用户名：
G039
密码：
CGS 密钥
登记者
9B
请求接入
后退
你有接入权限
前大门
你有接入权限
前门
发送请求到应用
通过文本发送请求
通过电话发送请求
车库
发送请求到应用
通过文本发送请求
通过电话发送请求
电梯
9C
密码
368083474
剩余时间
4:55
发送以解锁
我已经打开了锁
我无法打开锁

图9A-9C