

(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国际局

(43) 国际公布日
2019 年 2 月 21 日 (21.02.2019)



(10) 国际公布号
WO 2019/033840 A1

- (51) 国际专利分类号:
H04L 29/08 (2006.01) **G07C 9/00** (2006.01)
- (21) 国际申请号: PCT/CN2018/090666
- (22) 国际申请日: 2018 年 6 月 11 日 (11.06.2018)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201710703147.0 2017年8月16日 (16.08.2017) CN
- (71) 申请人: 格力电器(武汉)有限公司(GREE ELECTRIC APPLIANCES (WUHAN) CO., LTD) [CN/CN]; 中国湖北省武汉市经济技术开发区东风大道 888 号, Hubei 430000 (CN)。珠海格力电器股份有限公司(GREE ELECTRIC APPLIANCES, INC. OF ZHUHAI) [CN/

CN]; 中国广东省珠海市前山金鸡西路, Guangdong 519070 (CN)。

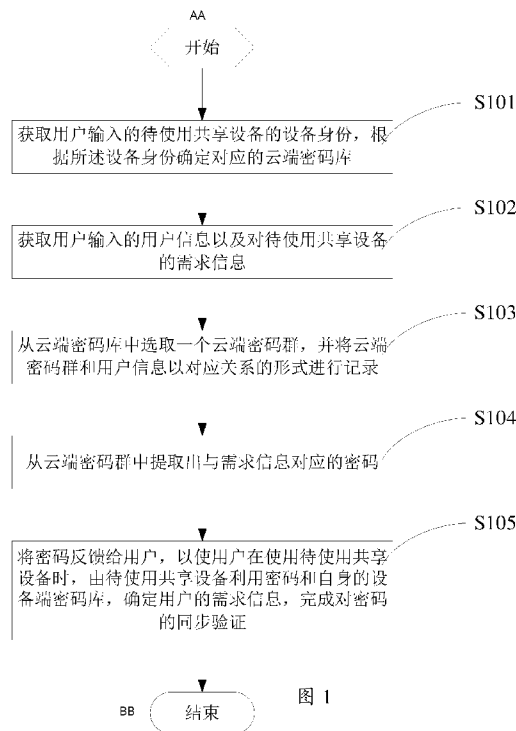
- (72) 发明人: 杨赛赛(YANG, Saisai); 中国广东省珠海市前山金鸡西路, Guangdong 519070 (CN)。苗岑岑(MIAO, Cencen); 中国广东省珠海市前山金鸡西路, Guangdong 519070 (CN)。李喜林(LI, Xilin); 中国广东省珠海市前山金鸡西路, Guangdong 519070 (CN)。

- (74) 代理人: 广州华进联合专利商标代理有限公司(ADVANCE CHINA IP LAW OFFICE); 中国广东省广州市天河区花城大道 85 号 3901 房, Guangdong 510623 (CN)。

- (81) 指定国(除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU,

(54) Title: PASSWORD AUTHENTICATION METHOD FOR SHARED DEVICE, SHARED DEVICE, CLOUD SERVER, AND SYSTEM

(54) 发明名称: 共享设备的密码验证方法、共享设备、云端服务器及系统



S101 Obtain a device identity of a shared device to be used that is input by a user, and determine, according to the device identity, a corresponding cloud password database

S102 Obtain user information and requirement information for the shared device to be used that are input by the user

S103 Select a cloud password group from the cloud password database, and record the cloud password group and the user information such that there is a correspondence therebetween

S104 Extract a password corresponding to the requirement information from the cloud password group

S105 Feed back the password to the user, such that when the user uses the shared device, the requirement information of the user is determined by the shared device by using the password and its own device password database, thereby completing synchronous verification of passwords

AA Start

BB End

图 1

(57) Abstract: Disclosed in the present application are a password authentication method for a shared device, a shared device, a cloud server, and a system. By adopting the same preset password generation rule for passwords in a corresponding cloud password database of a shared device in a cloud server and passwords in a device password database of the shared device, before using the shared device, a user can first extract a corresponding password from the cloud password database using requirement information for the device to be used, the password being obtained in advance by using the preset password generation rule for the requirement information, and then

CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(84) 指定国 (除另有指明, 要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:

— 包括国际检索报告 (条约第21条(3))。

input the password into the shared device. When the shared device finds a password corresponding to the password from its own device password database, the requirement information of the user can be determined by using the found password and the preset password generation rule, such that synchronous verification of passwords is completed without the need for connecting the cloud server and the shared device to a network.

(57) 摘要: 本申请公开了一种共享设备的密码验证方法、共享设备、云端服务器及系统, 通过将共享设备在云端服务器中对应的云端密码库中的密码, 和该共享设备的设备端密码库中的密码, 采用相同的预设密码生成规则, 使得用户在使用共享设备之前, 可以利用对待使用设备的需求信息, 首先从云端密码库提取对应的密码, 该密码预先对需求信息采用预设密码生成规则得到, 然后将该密码输入到共享设备, 当共享设备从自身的设备端密码库查找到与该密码对应的密码时, 可利用查找到的密码和预设的密码生成规则, 确定用户的需求信息, 从而实现在云端服务器和共享设备在无需连接网络的情况下, 完成对密码的同步验证。

共享设备的密码验证方法、共享设备、云端服务器及系统

相关申请

本申请要求 2017 年 08 月 16 日申请的，申请号为 201710703147.0，名称为“共享设备的密码验证方法、共享设备、云端服务器及系统”的中国专利申请的优先权，在此将其全文引入作为参考。

技术领域

本申请涉及共享设备技术领域，更具体的说，涉及一种共享设备的密码验证方法、共享设备、云端服务器及系统。

背景技术

近年来，各种具有自助付费功能的共享设备兴起，如共享单车、共享电动车、共享汽车、共享洗衣机等。这些共享设备的使用非常方便快捷，用户可以根据需要，下载相应的客户端并注册，在需要使用相应共享设备时，登录相应的客户端，输入待使用共享设备的编码获取解锁码，或者通过直接扫描待使用共享设备上的识别码的方式实现开锁。在使用完毕后，通过网上付费即可。

这些共享设备都有一个共同的特点：需要连接到互联网络或是与移动终端，如手机，建立近程无线通信才能实现与用户之间的信息同步，实现密码验证，因此，共享设备通常都具有无线模块。

由于共享设备的密码验证过程需基于网络实现，因此使得共享设备的使用受到网络限制，存在互联网不安全攻击的风险，因此，如何提供一种共享设备的密码验证方法，以使共享设备和云端服务器在无需连接网络的情况下，实现用户和共享设备之间密码的同步验证成为了本领域技术人员亟需解决的技术问题。

发明内容

有鉴于此，本申请公开一种共享设备的密码验证方法、共享设备、云端服务器及系统，以实现共享设备和云端服务器在无需连接网络的情况下，仍可实现用户和共享设备之间的密码同步验证过程。

一种共享设备的密码验证方法，应用于云端服务器，所述云端服务器具有多个云端密

码库，每一个云端密码库对应一个共享设备，所述方法包括：

获取用户输入的待使用共享设备的设备身份，根据所述设备身份确定对应的云端密码库；

获取所述用户输入的用户信息以及对所述待使用共享设备的需求信息；

从所述云端密码库中选取一个云端密码群，并将所述云端密码群和所述用户信息以对应关系的形式进行记录；

从所述云端密码群中提取出与所述需求信息对应的密码，其中，所述密码为预先对所述需求信息采用预设密码生成规则得到的密码；

将所述密码反馈给所述用户，以使所述用户在使用所述待使用共享设备时，由所述待使用共享设备利用所述密码，从自身的设备端密码库查找是否存储有与所述密码相同的密码，如果是，则利用查找到的密码和所述预设密码生成规则确定所述用户的所述需求信息，完成对所述密码的同步验证。

优选的，所述云端密码库包括多个云端密码群，每一个云端密码群对应一位用户，每一个云端密码群为按照预设密码生成规则针对共享设备在不同工作情况的排列组合下产生的所有密码的集合。

优选的，所述设备端密码库包括多个设备端密码群，每一个设备端密码群对应一位用户，每一个共享设备在设备端密码库存储的所有密码和与该共享设备相对应的云端密码库中的密码，均是对用户的需求信息采用相同的预设密码生成规则生成。

优选的，当所述云端服务器在所述用户完成付费后，提供密码给所述用户时，从所述云端密码群中提取出与所述需求信息对应的密码，具体包括：

从所述云端密码群中提取出与所述需求信息对应的需要所述用户支付的费用；

当检测到所述用户支付完所述费用后，从所述云端密码群中提取出与所述需求信息对应的密码。

优选的，当检测到所述用户支付完所述费用后，从所述云端密码群中提取出与所述需求信息对应的密码，具体包括：

当检测到所述用户支付完所述费用后，从所述云端密码群中提取出与所述需求信息对应的密码，并标记用户级别，其中，当多个用户需要支付费用时，所述用户级别根据用户完成支付的先后顺序确定，用户完成支付的时间越靠前，相对应的用户级别越高；

将所述密码反馈给所述用户，以使所述用户在使用所述待使用共享设备时，由所述待使用共享设备利用所述密码，从自身的设备端密码库查找是否存储有与所述密码相同的密码，如果是，则利用查找到的密码确定所述用户的所述需求信息，完成对所述密码的同步

验证，具体包括：

将所述密码反馈给所述用户，以使所述用户在使用所述待使用共享设备时，由所述待使用共享设备利用所述密码，从自身的设备端密码库查找是否存储有与所述密码相同的密码，如果是，则确定所述用户的用户级别和需求信息，完成对所述密码的同步验证。

优选的，所述云端密码库中所有的云端密码群和所述设备端密码库中所有的设备端密码群采用相同的密码分类分级方案。

一种共享设备的密码验证方法，应用于待使用共享设备，所述方法包括：

获取用户在云端密码库获取的密码，所述密码为预先对需求信息采用预设密码生成规则得到的密码，所述需求信息为所述用户对所述待使用共享设备的需求信息；

利用所述密码从自身的设备端密码库查找是否存储有与所述密码相同的密码；

如果是，则利用查找到的密码和所述预设密码生成规则确定所述用户的需求信息，完成对所述密码的同步验证。

优选的，所述云端密码库包括多个云端密码群，每一个云端密码群对应一位用户，每一个云端密码群为按照预设密码生成规则针对共享设备在不同工作情况的排列组合下产生的所有密码的集合。

优选的，所述设备端密码库包括多个设备端密码群，每一个设备端密码群对应一位用户，每一个共享设备在设备端密码库存储的所有密码和与该共享设备相对应的云端密码库中的密码，均是对用户的需求信息采用相同的预设密码生成规则生成。

优选的，所述利用所述密码从自身的设备端密码库查找是否存储有与所述密码相同的密码，具体包括：

利用所述密码从自身的设备端密码库的有效密码保留区放置的设备端密码群中，查找是否存储有与所述密码相同的密码，其中，所述有效密码保留区用于保留所述待使用共享设备已获取但未使用的密码。

优选的，所述利用所述密码从自身的设备端密码库查找是否存储有与所述密码相同的密码，具体包括：

当从自身的设备端密码库的有效密码保留区未查找到与所述密码相同的密码时，则从所述设备端密码库已产生的设备端密码群中，查找是否存储有与所述密码相同的密码。

优选的，当从所述设备端密码库已产生的设备端密码群中查找到与所述密码相同的密码，且云端密码群的级别、设备端密码群的级别和用户级别三者一致时，所述利用查找到的密码和所述预设密码生成规则确定所述用户的需求信息，完成对所述密码的同步验证，具体包括：

利用查找到的密码和所述预设密码生成规则确定所述用户的用户级别和需求信息，完成对所述密码的同步验证。

优选的，当完成对所述密码的同步验证之后，还包括：

将级别高于所述用户级别的未使用的设备端密码群放到所述有效密码保留区；

删除所有级别低于所述用户级别的设备端密码群。

优选的，在确定所述用户的需求信息，完成对所述密码的同步验证之后，还包括：

将验证成功的所述密码进行删除。

优选的，还包括：

当从所述设备端密码库未查找到与所述密码相同的密码时，输出提示信息，所述提示信息用于提示用户重新输入密码。

一种云端服务器，所述云端服务器具有多个云端密码库，每一个云端密码库对应一个共享设备，所述云端服务器包括：

第一获取单元，用于获取用户输入的待使用共享设备的设备身份，根据所述设备身份确定对应的云端密码库；

第二获取单元，用于获取所述用户输入的用户信息以及对所述待使用共享设备的需求信息；

选取单元，用于从所述云端密码库中选取一个云端密码群，并将所述云端密码群和所述用户信息以对应关系的形式进行记录；

提取单元，用于从所述云端密码群中提取出与所述需求信息对应的密码，其中，所述密码为预先对所述需求信息采用预设密码生成规则得到的密码；

反馈单元，用于将所述密码反馈给所述用户，以使所述用户在使用所述待使用共享设备时，由所述待使用共享设备利用所述密码，从自身的设备端密码库查找是否存储有与所述密码相同的密码，如果是，则利用查找到的密码和所述预设密码生成规则确定所述用户的所述需求信息，完成对所述密码的同步验证。

优选的，所述云端密码库包括多个云端密码群，每一个云端密码群对应一位用户，每一个云端密码群为按照预设密码生成规则针对共享设备在不同工作情况的排列组合下产生的所有密码的集合。

优选的，所述设备端密码库包括多个设备端密码群，每一个设备端密码群对应一位用户，每一个共享设备在设备端密码库存储的所有密码和与该共享设备相对应的云端密码库中的密码，均是对用户的需求信息采用相同的预设密码生成规则生成。

优选的，当所述云端服务器在所述用户完成付费后，提供密码给所述用户时，所述提

取单元包括:

第一提取子单元,用于从所述云端密码群中提取出与所述需求信息对应的需要所述用户支付的费用;

第二提取子单元,用于当检测到所述用户支付完所述费用后,从所述云端密码群提取出与所述需求信息对应的密码。

优选的,所述第二提取子单元具体用于:

当检测到所述用户支付完所述费用后,从所述云端密码群中提取出与所述需求信息对应的密码,并标记用户级别,其中,当多个用户需要支付费用时,所述用户级别根据用户完成支付的先后顺序确定,用户完成支付的时间越靠前,相对应的用户级别越高;

所述反馈单元具体用于:

将所述密码反馈给所述用户,以使所述用户在使用所述待使用共享设备时,由所述待使用共享设备利用所述密码,从自身的设备端密码库查找是否存储有与所述密码相同的密码,如果是,则确定所述用户的用户级别和需求信息,完成对所述密码的同步验证。

优选的,所述云端密码库中所有的云端密码群和所述设备端密码库中所有的设备端密码群采用相同的密码分类分级方案。

一种共享设备,包括:

第三获取单元,用于获取用户在云端密码库获取的密码,所述密码为预先对需求信息采用预设密码生成规则得到的密码,所述需求信息为所述用户对所述待使用共享设备的需求信息;

查找单元,用于利用所述密码从自身的设备端密码库查找是否存储有与所述密码相同的密码;

验证单元,用于利用查找到的密码和所述预设密码生成规则确定所述用户的需求信息,完成对所述密码的同步验证。

优选的,所述云端密码库包括多个云端密码群,每一个云端密码群对应一位用户,每一个云端密码群为按照预设密码生成规则针对共享设备在不同工作情况的排列组合下产生的所有密码的集合。

优选的,所述设备端密码库包括多个设备端密码群,每一个设备端密码群对应一位用户,每一个共享设备在设备端密码库存储的所有密码和与该共享设备相对应的云端密码库中的密码,均是对用户的需求信息采用相同的预设密码生成规则生成。

优选的,所述查找单元具体用于:

利用所述密码从自身的设备端密码库的有效密码保留区放置的设备端密码群中,查找

是否存储有与所述密码相同的密码，其中，所述有效密码保留区用于保留所述待使用共享设备已获取但未使用的密码。

优选的，所述查找单元具体用于：

当从自身的设备端密码库的有效密码保留区未查找到与所述密码相同的密码时，则从所述设备端密码库已产生的设备端密码群中，查找是否存储有与所述密码相同的密码。

优选的，当从所述设备端密码库已产生的设备端密码群中查找到与所述密码相同的密码，且云端密码群的级别、设备端密码群的级别和用户级别三者一致时，所述验证单元具体用于：

利用查找到的密码和所述预设密码生成规则确定所述用户的用户级别和需求信息，完成对所述密码的同步验证。

优选的，还包括：

放置单元，用于当完成对所述密码的同步验证之后，将级别高于所述用户级别的未使用的设备端密码群放到所述有效密码保留区；

第一删除单元，用于删除所有级别低于所述用户级别的设备端密码群。

优选的，还包括：

第二删除单元，用于在确定所述用户的需求信息，完成对所述密码的同步验证之后，将验证成功的所述密码进行删除。

优选的，还包括：

输出单元，用于当从所述设备端密码库未查找到与所述密码相同的密码时，输出提示信息，所述提示信息用于提示用户重新输入密码。

一种共享设备的密码验证系统，包括上述所述的云端服务器和至少一个上述所述的共享设备。

从上述的技术方案可知，本申请公开了一种共享设备的密码验证方法、共享设备、云端服务器及系统，通过将共享设备在云端服务器中对应的云端密码库中的密码，和该共享设备的设备端密码库中的密码，采用相同的预设密码生成规则，使得用户在使用共享设备之前，可以利用对待使用设备的需求信息，首先从云端密码库提取对应的密码，该密码预先对需求信息采用预设密码生成规则得到，然后将该密码输入到共享设备，当共享设备从自身的设备端密码库查找到与该密码对应的密码时，可利用查找到的密码和预设的密码生成规则，确定用户的需求信息，从而完成对密码的同步验证。因此，本申请实现了在云端服务器和共享设备在无需连接网络的情况下，基于相同的密码生成规则，实现了用户和共享设备之间的密码同步验证过程，从而使得共享设备的使用不再受到网络限制，进而有效

避免了互联网不安全攻击的风险。

附图说明

为了更清楚地说明本申请实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本申请的实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据公开的附图获得其他的附图。

图 1 为本申请实施例公开的一种基于云端服务器侧的共享设备的密码验证方法流程图；

图 2 为本申请实施例公开的一种费用、密码、云端密码群和云端密码库的对应关系示意图；

图 3 为本申请实施例公开的一种云端服务器和一个共享设备的对应关系示意图；

图 4 为本申请实施例公开的一种基于共享设备侧的共享设备的密码验证方法流程图；

图 5 为本申请实施例公开的一种云端服务器的结构示意图；

图 6 为本申请实施例公开的一种共享设备的结构示意图。

具体实施方式

下面将结合本申请实施例中的附图，对本申请实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本申请一部分实施例，而不是全部的实施例。基于本申请中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本申请保护的范围。

本申请实施例公开了一种共享设备的密码验证方法、共享设备、云端服务器及系统，以实现共享设备和云端服务器在无需连接网络的情况下，仍可实现用户和共享设备之间的密码同步验证过程。

参见图 1，本申请一实施例公开的一种共享设备的密码验证方法流程图，该方法应用于云端服务器，该云端服务器与至少一个共享设备成对应关系，该云端服务器具有多个云端密码库，每一个云端密码库对应一个共享设备，所述方法包括步骤：

步骤 S101、获取用户输入的待使用共享设备的设备身份，根据所述设备身份确定对应的云端密码库；

在实际应用中，用户可以通过手机、IPAD 等终端扫描共享设备的二维码来获取共享设备的设备身份，该设备身份也即设备标识。当然，用户还可以采用其它的方式获取共享

设备的设备身份，如通过将共享设备上印制的身份码输入电脑来获取共享设备的设备身份。

其中，每一个共享设备都有与之唯一对应的设备身份。

步骤 S102、获取用户输入的用户信息以及对待使用共享设备的需求信息；

具体的，用户信息具体指的是用户的身份信息，如身份证号码。

对于共享设备的需求信息，举例说明，假设，共享设备为共享洗衣机，则用户对共享洗衣机的需求信息包括：洗衣时长、漂洗次数、洗涤温度、转速等等。

步骤 S103、从所述云端密码库中选取一个云端密码群，并将所述云端密码群和所述用户信息以对应关系的形式进行记录；

本实施例中，一个云端密码库包括多个云端密码群，每一个云端密码群对应一位用户，每一个云端密码群为按照预设密码生成规则针对共享设备在不同工作情况的排列组合下产生的所有密码的集合，也即每一个云端密码群中包含用户所需求使用共享设备的所有情况。举例说明，假设共享设备为共享洗衣机，用户对共享洗衣机的需求信息也即共享洗衣机的工作情况为：洗衣时长为 30 分钟，洗衣模式为：两次漂洗加一次脱水，衣物类型为：衬衫，根据这些需求信息以及预设密码生成规则如密码生成公式，得到一个与该需求信息唯一对应的一个密码。

通过将共享洗衣机按照预设密码生成规则在不同工作情况下的排列组合产生所有密码的集合，也即得到一个云端密码群。

当云端密码群在云端密码库中按顺序排列时，可将排列最前面的云端密码群作为选用的云端密码群，当然，也可以随机选择一个云端密码群。

其中，将云端密码群和用户信息以对应关系的形式进行记录的目的是：实现共享设备使用的实名制，以避免向未达到年龄要求的用户提供服务，如共享单车的使用用户需年满 12 周岁，同时为后续为用户购买人身意外伤害险和第三者责任险等提供条件。

在实际应用中，可以对云端密码库中包含的各个云端密码群设置不同的级别，同时，对用户设置不同的等级，如根据用户历次使用共享设备的总次数确定用户的级别，用户使用的次数越多，用户的级别越高，同一级别的用户和云端密码群相对应。

因此，本步骤的执行过程具体为：首先确定待使用共享设备对应的多个云端密码群，其次，根据用户信息确定用户级别，并根据用户级别确定对应的云端密码群。

步骤 S104、从云端密码群中提取出与需求信息对应的密码；

其中，所述密码为预先对所述需求信息采用预设密码生成规则得到的密码，也即该密码是按照预设密码生成规则针对共享设备在不同的工作情况的排列组合下产生的，因此，

根据需求信息也即共享设备的工作情况，可从云端密码群中提取出对应的密码。

步骤 S105、将密码反馈给用户，以使用户在使用待使用共享设备时，由待使用共享设备利用密码和自身的设备端密码库，确定用户的需求信息，完成对密码的同步验证。

具体的，云端密码库将查找到的密码反馈给用户，用户在使用待使用共享设备时，向待使用共享设备输入该密码，待使用共享设备利用密码从自身的设备端密码库查找是否存储有与用户输入的密码相同的密码，如果是，则利用查找到的密码和所述预设密码生成规则确定用户的需求信息，完成对密码的同步验证。

其中，所述设备端密码库包括多个设备端密码群，每一个设备端密码群对应一位用户，每一个共享设备在设备端密码库存储的所有密码和与该共享设备相对应的云端密码库中的密码，均是对用户的需求信息采用相同的预设密码生成规则生成，这样，共享设备根据用户从云端密码库获取的密码，即可确定用户的需求信息。

综上，本申请公开的共享设备的密码验证方法，通过将共享设备在云端服务器中对应的云端密码库中的密码，和该共享设备的设备端密码库中的密码，采用相同的预设密码生成规则，使得用户在使用共享设备之前，可以利用对待使用设备的需求信息，首先从云端密码库提取对应的密码，该密码预先对需求信息采用预设密码生成规则得到，然后将该密码输入到共享设备，当共享设备从自身的设备端密码库查找到与该密码对应的密码时，可利用查找到的密码和预设的密码生成规则，确定用户的需求信息，从而完成对密码的同步验证。因此，本申请实现了在云端服务器和共享设备在无需连接网络的情况下，基于相同的密码生成规则，实现了用户和共享设备之间的密码同步验证过程，从而使得共享设备的使用不再受到网络限制，进而有效避免了互联网不安全攻击的风险。

另外，由于本申请公开的方法无需共享设备与云端服务器之间建立网络连接，因此，相比传统方案而言，本申请还省去了设置在共享设备上的无线模块，从而节约了共享设备的硬件成本。

可以理解，不同的共享设备对付费的时间要求可不同，如共享洗衣机，当用户确定对共享洗衣机的需求信息后，共享洗衣机就可以根据这些需求信息生成相应的费用；又比如共享单车，由于提前无法获知用户的使用时间，因此无法提前确定用户的费用，对于这类共享设备，可以在用户使用完成之后再付费。

对于用户在使用完共享设备再付费的方案，可参见现有方案，此处不再赘述。

对于用户先付费再使用共享设备的方案，可参见下述示例。

上述实施例中，当云端服务器在用户完成付费后，才提供密码给所述用户时，步骤 S104 具体包括：

从云端密码群中提取出与需求信息对应的需要用户支付的费用；

当检测到用户支付完费用后，从云端密码群中提取出与需求信息对应的密码。

基于本实施例可以看出，费用和密码都是根据用户需求从云端密码群提取出来的，例如共享洗衣机，云端服务器根据用户选择的洗衣时长、转速、洗涤温度，可以从云端密码群查找到一个相对应的需要用户支付的费用，在用户支付成功后，云端服务器会提供给用户一个相对应的密码。

其中，费用、密码、云端密码群和云端密码库的对应关系可参见图 2 所示的示意图，图 2 中，云端密码库包括多个云端密码群，如云端密码群 1、云端密码群 2、……云端密码群 X，每一个云端密码群对应一个用户，多个用户对应多个云端密码群，在实际应用中，所有的云端密码群可以按照级别先后排列组合成云端密码库，每一个云端密码群为按照预设密码生成规则针对共享设备在不同工作情况的排列组合下产生的所有密码的集合，也即每一个云端密码群中包含用户所需求使用共享设备的所有情况，比如，图 2 中的云端密码群 X，共享设备不同的工作情况包括因素：（1）共享设备的使用时长，如 5 分钟、10 分钟、20 分钟；（2）数量，以共享洗衣机为例，该数量可指用户需洗衣物的数量，如 1、2、3；（3）变量（如图 2 中的变量 3、变量 N）是指影响共享设备工作模式和费用的因素变量，不同的时长可以认为是某个变量下的一个元素，一种变量可以包括多种元素，如元素 a、元素 b、元素 c 等。不同因素的排列组合产生一个密码和与该密码相对应的唯一的费用，如图 2 中，密码 a 与费用 a 对应，密码 b 与费用 b 对应，密码 c 与费用 c 对应，密码 d 与费用 d 对应，密码 e 与费用 e 对应。

需要说明的是，云端服务器与至少一个共享设备成对应关系，云端服务器和每一个共享设备都可以组成一个系统，云端服务器和多个共享设备组成多个系统，在实际应用中，同一系统要保证设备端密码库和相对应的云端密码库所采用的预设密码生成规则（包括密码生成的算法和加密原则）一致，不同的系统之间的预设密码生成规则可以不同。并且，还需保证云端密码库连续产生的一定数量的云端密码群中的密码不能重复。

较优的，上述实施例中，云端密码库中所有的云端密码群和设备端密码库中所有的设备端密码群可采用相同的密码分类分级方案，也就是说，针对同一用户的同一需求信息，对应的云端密码群和设备端密码群的级别相同，并且云端密码群中的密码和设备端密码群中的密码所采用的预设密码生成规则相同，但云端密码群中的密码和设备端密码群中密码所产生的时间可以相同，也可以不同。

为方便查找密码，在实际应用中，对于先付费再使用共享设备的方案，可以根据用户完成支付的先后顺序，确定用户级别，当多个用户需要支付费用时，用户支付的时间越靠

前，对应的用户级别越高，用户级别和相对应的云端密码群的级别、设备端密码群的级别相同。

参见图 3，本申请一实施例公开的一种云端服务器和一个共享设备的对应关系示意图，其中，图 3 中仅示出一个云端服务器和一个共享设备的对应关系，在实际应用中，可以一个云端服务器对应多个共享设备，多个共享设备在云端服务器中对应的云端密码库分开管理，互补影响。

结合图 2 和图 3 可知，当用户向云端密码库输入不同的需求信息时，如时间、工作模式、数量、变量三、变量四等，可以从云端密码库获取不同的密码，其中，不同的用户会获取不同的密码，如用户 1 获取密码 1，用户 2 获取密码 2，用户 3 获取密码 3，用户 4 获取密码 4，用户 5 获取密码 5 等。

在实际应用中，可以将云端密码群进行级别划分，沿图 3 中箭头所示方向，云端密码群的等级逐渐升高，由于一个云端密码群对应一位用户，每一位用户都会从相对应的云端密码群获取密码，因此，图 3 所示实施例中，密码 1~密码 5 的等级逐渐升高。

在共享设备侧，设备端密码库包括多个设备端密码群，如设备端密码群 1~5，每一个设备端密码群对应一位用户，如设备端密码群 5 与用户 5 对应，设备端密码群中的密码和云端密码群中的密码所采用的预设密码生成规则相同。

若对云端密码群进行级别划分，那么，相应的，也可对设备端密码群进行级别划分，沿图 3 中箭头所示方向，设备端密码群的等级逐渐升高。

其中，用户等级、设备端密码群等级和云端密码群等级三者的等级相同。

在实际应用中，同级用户使用同级设备端密码群，各同级设备端密码群可正常轮换，当然，在一些情况下，用户也可以越级使用设备端密码群，如图 3 中用户 2 正常应使用设备端密码群 2，然而，在一些情况下，用户 2 也可以使用设备端密码群 3，此时，可将低等级的设备端密码群 1 和设备端密码群 2 放置到有效密码保留区，以下次使用。

为进一步优化上述实施例，当检测到用户支付完费用后，从云端密码群提取出与需求信息对应的密码的过程，具体可以包括：

当检测到用户支付完所述费用后，从云端密码群中提取出与所述需求信息对应的密码，并标记用户级别，其中，当多个用户需要支付费用时，所述用户级别根据用户完成支付的先后顺序确定，用户完成支付的时间越靠前，相对应的用户级别越高。

需要说明的是，云端服务器提供给用户的密码，是从与用户级别对应的云端密码群中根据用户输入的需求信息提取出来的，例如，共享洗衣机，用户的需求信息包括：洗涤时间为 30 分钟，漂洗 2 次，脱水 1 次，云端服务器根据这些需求信息，从与用户级别对应

的云端密码群中提取对应的密码。

相应的，步骤 S105 具体包括：

将密码反馈给用户，以使用户在使用所述待使用共享设备时，由所述待使用共享设备利用所述密码，从自身的设备端密码库查找是否存储有与所述密码相同的密码，如果是，则确定所述用户的用户级别和需求信息，完成对所述密码的同步验证。

其中，用户在向共享设备输入密码时，可以以数字的形式输入，或由共享设备根据用户支付费用后所产生的二维码凭证自助识别，或是以口令语音识别方式输入等。

需要说明的是，密码在设备端密码群中是不分级别排列的，只有密码被用户输入到共享设备，并确定使用后才有级别之分，且密码的级别和对应的设备端密码群的级别相同。

参见图 4，本申请另一实施例公开的一种共享设备的密码验证方法流程图，该方法应用于待使用共享设备，该待使用共享设备如共享单车、共享电动车、共享洗衣机等，该方法包括步骤：

步骤 S201、获取用户在云端密码库获取的密码；

其中，所述密码为预先对需求信息采用预设密码生成规则得到的密码，所述需求信息为所述用户对所述待使用共享设备的需求信息。

用户在云端密码库获取密码的过程可参见图 1 所示实施例，此处不再赘述。

步骤 S202、利用密码从自身的设备端密码库查找是否存储有与密码相同的密码；

其中，设备端密码库包括多个设备端密码群，每一个设备端密码群对应一位用户，每一个共享设备在设备端密码库存储的所有密码和与该共享设备相对应的云端密码库中的密码，均是对用户的需求信息采用相同的预设密码生成规则生成，这样，共享设备根据用户从云端密码库获取的密码和预设密码生成规则，即可确定用户的需求信息。

本步骤中，待使用共享设备确定自身设备端密码库是否存储有与用户输入的密码相同的密码的目的是：判断用户输入的密码是否为有效密码。

步骤 S203、如果是，则利用查找到的密码和所述预设密码生成规则确定用户的需求信息，完成对密码的同步验证。

其中，所述云端密码库包括多个云端密码群，每一个云端密码群对应一位用户，且每一个云端密码群为按照预设密码生成规则针对共享设备在不同工作情况的排列组合下产生的所有密码的集合。

综上，本申请公开的共享设备的密码验证方法，通过将共享设备在云端服务器中对应的云端密码库中的密码，和该共享设备的设备端密码库中的密码，采用相同的预设密码生成规则，使得用户在使用共享设备之前，可以利用对待使用设备的需求信息，首先从云端

密码库提取对应的密码，该密码预先对需求信息采用预设密码生成规则得到，然后将该密码输入到共享设备，当共享设备从自身的设备端密码库查找到与该密码对应的密码时，可利用查找到的密码和预设的密码生成规则，确定用户的需求信息，从而完成对密码的同步验证。因此，本申请实现了在云端服务器和共享设备在无需连接网络的情况下，基于相同的密码生成规则，实现了用户和共享设备之间的密码同步验证过程，从而使得共享设备的使用不再受到网络限制，进而有效避免了互联网不安全攻击的风险。

另外，由于本申请公开的方法无需共享设备与云端服务器之间建立网络连接，因此，相比传统方案而言，本申请还省去了设置在共享设备上的无线模块，从而节约了共享设备的硬件成本。

其中，当从所述设备端密码库未查找到与所述密码相同的密码时，输出提示信息，所述提示信息用于提示用户重新输入密码。

如图3所示，在实际应用中，可以在设备端密码库设置有效密码保留区，当待使用共享设备需要确定用户输入的密码是否存储时，可优先在有效密码保留区查找，若在有效密码保留区未查找到，则从设备端密码库已产生的未位于有效密码保留区的设备端密码群中查找。

其中，有效密码保留区主要用于保留待使用共享设备已获取但未使用的密码。

因此，为进一步优化上述实施例，步骤S202具体可以包括：

利用密码从自身的设备端密码库的有效密码保留区放置的设备端密码群中，查找是否存储有与所述密码相同的密码。

步骤S202具体还可以包括：

当从自身的设备端密码库的有效密码保留区未查找到与所述密码相同的密码时，则从所述设备端密码库已产生的设备端密码群中，查找是否存储有与所述密码相同的密码。

在实际应用中，对于先付费再使用共享设备的方案，可以根据用户完成支付的先后顺序，确定用户级别，当多个用户需要支付费用时，用户支付的时间越靠前，对应的用户级别越高，用户级别、云端密码群的级别和设备端密码群的级别三者一致。

因此，云端服务器在提取出密码，并且对用户级别进行标记后，那么，待使用共享设备可以根据与用户提供的密码匹配的密码所在的设备端密码群的级别，可以确定用户级别。

所以，当从所述设备端密码库已产生的设备端密码群中查找到与所述密码相同的密码，上述实施例中的步骤S203具体可以包括：

利用查找到的密码和所述预设密码生成规则确定所述用户的用户级别和需求信息，完

成对所述密码的同步验证。

需要说明的是，有效密码保留区的密码被使用时，不对正常级别的密码轮换产生影响，有效密码保留区中的密码直到被使用时才会消失。

当完成对密码的同步验证之后，可将级别高于用户级别的未使用的设备端密码群放到所述有效密码保留区，并删除所有级别低于所述用户级别的设备端密码群。

其中，云端密码库中的云端密码群和设备端密码库中的设备端密码群是根据预设规则逐渐产生的，并以设定规则逐渐消除低等级的密码群，以保证云端密码库的云端密码群和设备端密码库中的设备端密码群在一定数量范围内，且不重复。

云端密码群可以在提供给用户密码或用户完成一次支付行为后，增加一个或多个云端密码群，也可以通过日期，一定天数增加一定数据的云端密码群，或是根据用户使用的频繁程度，确定密码产生的数量，无效云端密码群的去除可采用以下方式：设定云端密码群有效期，超期后自动删除；在用户完成自助服务后，并反馈完成后，对所使用的云端密码群进行删除；也可以采用多种方式混合判断。

设备端密码群是否需要增加，以增加的数量以用户使用的次数、使用的时间间隔、现有有效设备端密码群数量、共享设备的工作特点、用户输入的密码等级等中的一种或多种混合方式进行确定，无效密码的消除以用户使用过自动删除为准。

经过一段使用时间后，当共享设备已获取但未用的密码增加时，有效密码保留区中的容量会越来越大，当增加到一定数量后以一定方式进行消除，以共享设备的工作特点，用户使用此次，有效密码保留区中的密码等级综合判断。

上述实施例，当确定用户的需求信息，完成对密码的同步验证后，还包括：

将验证成功的密码进行删除。

需要说明的是，本申请中，当共享设备在工作过程中出现异常情况，如断电时，共享设备会把异常情况之前的信息进行存储，待恢复正常后，继续之前的工作，直至完成本次服务。

与上述方法实施例相对应，本申请还公开了一种云端服务器和一种共享设备，具体参见下述描述。

参见图 5，本申请一实施例公开的一种云端服务器的结构示意图，该云端服务器与至少一个共享设备成对应关系，该云端服务器具有多个云端密码库，每一个云端密码库对应一个共享设备，该云端服务器包括：

第一获取单元 301，用于获取用户输入的待使用共享设备的设备身份，根据所述设备身份确定对应的云端密码库；

在实际应用中，用户可以通过手机、IPAD 等终端扫描共享设备的二维码来获取共享设备的设备身份，该设备身份也即设备标识。当然，用户还可以采用其它的方式获取共享设备的设备身份，如通过将共享设备上印制的身份码输入电脑来获取共享设备的设备身份。

其中，每一个共享设备都有与之唯一对应的设备身份。

第二获取单元 302，用于获取所述用户输入的用户信息以及对所述待使用共享设备的需求信息；

具体的，用户信息具体指的是用户的身份信息，如身份证号码。

对于共享设备的需求信息，举例说明，假设，共享设备为共享洗衣机，则用户对共享洗衣机的需求信息包括：洗衣时长、漂洗次数、洗涤温度、转速等等。

选取单元 303，用于从所述云端密码库中选取一个云端密码群，并将所述云端密码群和所述用户信息以对应关系的形式进行记录；

本实施例中，一个云端密码库包括多个云端密码群，每一个云端密码群对应一位用户，每一个云端密码群为按照预设密码生成规则针对共享设备在不同工作情况的排列组合下产生的所有密码的集合，也即每一个云端密码群中包含用户所需求使用共享设备的所有情况。举例说明，假设共享设备为共享洗衣机，用户对共享洗衣机的需求信息也即共享洗衣机的工作情况为：洗衣时长为 30 分钟，洗衣模式为：两次漂洗加一次脱水，衣物类型为：衬衫，根据这些需求信息以及预设密码生成规则如密码生成公式，得到一个与该需求信息唯一对应的一个密码。

通过将共享洗衣机按照预设密码生成规则在不同工作情况下的排列组合产生所有密码的集合，也即得到一个云端密码群。

当云端密码群在云端密码库中按顺序排列时，可将排列最前面的云端密码群作为选用的云端密码群，当然，也可以随机选择一个云端密码群。

其中，将云端密码群和用户信息以对应关系的形式进行记录的目的是：实现共享设备使用的实名制，以避免向未达到年龄要求的用户提供服务，如共享单车的使用用户需年满 12 周岁，同时为后续为用户购买人身意外伤害险和第三者责任险等提供条件。

在实际应用中，可以对云端密码库中包含的各个云端密码群设置不同的级别，同时，对用户设置不同的等级，如根据用户历次使用共享设备的总次数确定用户的级别，用户使用的次数越多，用户的级别越高，同一级别的用户和云端密码群相对应。

因此，选取单元 303 执行过程具体为：首先确定待使用共享设备对应的多个云端密码群，其次，根据用户信息确定用户级别，并根据用户级别确定对应的云端密码群。

提取单元 304，用于从所述云端密码群中提取出与所述需求信息对应的密码；

其中，所述密码为预先对所述需求信息采用预设密码生成规则得到的密码，也即该密码是按照预设密码生成规则针对共享设备在不同的工作情况的排列组合下产生的，因此，根据需求信息也即共享设备的工作情况，可从云端密码群中提取出对应的密码。

反馈单元 305，用于将所述密码反馈给所述用户，以使所述用户在使用所述待使用共享设备时，由所述待使用共享设备利用所述密码，从自身的设备端密码库查找是否存储有与所述密码相同的密码，如果是，则利用查找到的密码和所述预设密码生成规则确定所述用户的所述需求信息，完成对所述密码的同步验证。

具体的，云端密码库将查找到的密码反馈给用户，用户在使用待使用共享设备时，向待使用共享设备输入该密码，待使用共享设备利用密码从自身的设备端密码库查找是否存储有与用户输入的密码相同的密码，如果是，则利用查找到的密码和所述预设密码生成规则确定用户的需求信息，完成对密码的同步验证。

其中，所述设备端密码库包括多个设备端密码群，每一个设备端密码群对应一位用户，每一个共享设备在设备端密码库存储的所有密码和与该共享设备相对应的云端密码库中的密码，均是对用户的需求信息采用相同的预设密码生成规则生成，这样，共享设备根据用户从云端密码库获取的密码，即可确定用户的需求信息。

综上，本申请公开的云端服务器，通过将共享设备在云端服务器中对应的云端密码库中的密码，和该共享设备的设备端密码库中的密码，采用相同的预设密码生成规则，使得用户在使用共享设备之前，可以利用对待使用设备的需求信息，首先从云端密码库提取对应的密码，该密码预先对需求信息采用预设密码生成规则得到，然后将该密码输入到共享设备，当共享设备从自身的设备端密码库查找到与该密码对应的密码时，可利用查找到的密码和预设的密码生成规则，确定用户的需求信息，从而完成对密码的同步验证。因此，本申请实现了在云端服务器和共享设备在无需连接网络的情况下，基于相同的密码生成规则，实现了用户和共享设备之间的密码同步验证过程，从而使得共享设备的使用不再受到网络限制，进而有效避免了互联网不安全攻击的风险。

另外，由于本申请公开的方法无需共享设备与云端服务器之间建立网络连接，因此，相比传统方案而言，本申请还省去了设置在共享设备上的无线模块，从而节约了共享设备的硬件成本。

可以理解，不同的共享设备对付费的时间要求可不同，如共享洗衣机，当用户确定对共享洗衣机的需求信息后，共享洗衣机就可以根据这些需求信息生成相应的费用；又比如共享单车，由于提前无法获知用户的使用时间，因此无法提前确定用户的费用，对于这类

共享设备，可以在用户使用完成之后再付费。

对于用户在使用完共享设备再付费的方案，可参见现有方案，此处不再赘述。

对于用户先付费再使用共享设备的方案，可参见下述示例。

上述实施例中，当云端服务器在用户完成付费后，才提供密码给所述用户时，

提取单元 304 包括：

第一提取子单元，用于从所述云端密码群中提取出与所述需求信息对应的需要所述用户支付的费用；

第二提取子单元，用于当检测到所述用户支付完所述费用后，从所述云端密码群提取出与所述需求信息对应的密码。

基于本实施例可以看出，费用和密码都是根据用户需求从云端密码群提取出来的，例如共享洗衣机，云端服务器根据用户选择的洗衣时长、转速、洗涤温度，可以从云端密码群查找到一个相对应的需要用户支付的费用，在用户支付成功后，云端服务器会提供给用户一个相对应的密码。

其中，费用、密码、云端密码群和云端密码库的对应关系可参见图 2 所示的示意图以及相关描述。

需要说明的是，云端服务器与至少一个共享设备成对应关系，云端服务器和每一个共享设备都可以组成一个系统，云端服务器和多个共享设备组成多个系统，在实际应用中，同一系统要保证设备端密码库和相对应的云端密码库所采用的预设密码生成规则（包括密码生成的算法和加密原则）一致，不同的系统之间的预设密码生成规则可以不同。并且，还需保证云端密码库连续产生的一定数量的云端密码群中的密码不能重复。

较优的，上述实施例中，云端密码库中所有的云端密码群和设备端密码库中所有的设备端密码群可采用相同的密码分类分级方案，也就是说，针对同一用户的同一需求信息，对应的云端密码群和设备端密码群的级别相同，并且云端密码群中的密码和设备端密码群中的密码所采用的预设密码生成规则相同，但云端密码群中的密码和设备端密码群中密码所产生的时间可以相同，也可以不同。

为方便查找密码，在实际应用中，对于先付费再使用共享设备的方案，可以根据用户完成支付的先后顺序，确定用户级别，当多个用户需要支付费用时，用户支付的时间越靠前，对应的用户级别越高，用户级别和相对应的云端密码群的级别、设备端密码群的级别相同。

云端服务器和共享设备的对应关系可参见图 3 以及相关描述，此处不再追溯。

为进一步优化上述实施例，第二提取子单元具体用于：

当检测到所述用户支付完所述费用后，从所述云端密码群中提取出与所述需求信息对应的密码，并标记用户级别，其中，当多个用户需要支付费用时，所述用户级别根据用户完成支付的先后顺序确定，用户完成支付的时间越靠前，相对应的用户级别越高；

反馈单元 305 具体用于：

所述将所述密码反馈给所述用户，以使所述用户在使用所述待使用共享设备时，由所述待使用共享设备利用所述密码，从自身的设备端密码库查找是否存储有与所述密码相同的密码，如果是，则确定所述用户的用户级别和需求信息，完成对所述密码的同步验证。

其中，用户在向共享设备输入密码时，可以以数字的形式输入，或由共享设备根据用户支付费用后所产生的二维码凭证自助识别，或是以口令语音识别方式输入等。

需要说明的是，密码在设备端密码群中是不分级别排列的，只有密码被用户输入到共享设备，并确定使用后才有级别之分，且密码的级别和对应的设备端密码群的级别相同。

参见图 6，本申请一实施例公开的一种共享设备的结构示意图，该共享如共享单车、共享电动车、共享洗衣机等，共享设备包括：

第三获取单元 401，用于获取用户在云端密码库获取的密码，所述密码为预先对需求信息采用预设密码生成规则得到的密码，所述需求信息为所述用户对所述待使用共享设备的需求信息；

查找单元 402，用于利用所述密码从自身的设备端密码库查找是否存储有与所述密码相同的密码；

其中，设备端密码库包括多个设备端密码群，每一个设备端密码群对应一位用户，每一个共享设备在设备端密码库存储的所有密码和与该共享设备相对应的云端密码库中的密码，均是对用户的需求信息采用相同的预设密码生成规则生成，这样，共享设备根据用户从云端密码库获取的密码和预设密码生成规则，即可确定用户的需求信息。

验证单元 403，用于利用查找到的密码和所述预设密码生成规则确定所述用户的需求信息，完成对所述密码的同步验证。

其中，所述云端密码库包括多个云端密码群，每一个云端密码群对应一位用户，每一个云端密码群为按照预设密码生成规则针对共享设备在不同工作情况的排列组合下产生的所有密码的集合；所述设备端密码库包括多个设备端密码群，每一个设备端密码群对应一位用户，每一个共享设备在设备端密码库存储的所有密码和与该共享设备相对应的云端密码库中的密码，均是对用户的需求信息采用相同的预设密码生成规则生成，这样，共享设备根据用户从云端密码库获取的密码，即可确定用户的需求信息。

综上，本申请公开的共享设备，通过将共享设备在云端服务器中对应的云端密码库中

的密码, 和该共享设备的设备端密码库中的密码, 采用相同的预设密码生成规则, 使得用户在使用共享设备之前, 可以利用对待使用设备的需求信息, 首先从云端密码库提取对应的密码, 该密码预先对需求信息采用预设密码生成规则得到, 然后将该密码输入到共享设备, 当共享设备从自身的设备端密码库查找到与该密码对应的密码时, 可利用查找到的密码和预设的密码生成规则, 确定用户的需求信息, 从而完成对密码的同步验证。因此, 本申请实现了在云端服务器和共享设备在无需连接网络的情况下, 基于相同的密码生成规则, 实现了用户和共享设备之间的密码同步验证过程, 从而使得共享设备的使用不再受到网络限制, 进而有效避免了互联网不安全攻击的风险。

另外, 由于本申请公开的方法无需共享设备与云端服务器之间建立网络连接, 因此, 相比传统方案而言, 本申请还省去了设置在共享设备上的无线模块, 从而节约了共享设备的硬件成本。

为进一步优化上述实施例, 还包括: 输出单元, 用于当从所述设备端密码库未查找到与所述密码相同的密码时, 输出提示信息, 所述提示信息用于提示用户重新输入密码。

如图 3 所示, 在实际应用中, 可以在设备端密码库设置有效密码保留区, 当待使用共享设备需要确定用户输入的密码是否存储时, 可优先在有效密码保留区查找, 若在有效密码保留区未查找到, 则从设备端密码库已产生的未位于有效密码保留区的设备端密码群中查找。

其中, 有效密码保留区主要用于保留待使用共享设备已获取但未使用的密码。

因此, 为进一步优化上述实施例, 查找单元 402 具体可以用于:

利用所述密码从自身的设备端密码库的有效密码保留区放置的设备端密码群中, 查找是否存储有与所述密码相同的密码, 其中, 所述有效密码保留区用于保留所述待使用共享设备已获取但未使用的密码。

查找单元 402 具体还可以用于:

当从自身的设备端密码库的有效密码保留区未查找到与所述密码相同的密码时, 则从所述设备端密码库已产生的设备端密码群中, 查找是否存储有与所述密码相同的密码。

在实际应用中, 对于先付费再使用共享设备的方案, 可以根据用户完成支付的先后顺序, 确定用户级别, 当多个用户需要支付费用时, 用户支付的时间越靠前, 对应的用户级别越高, 用户级别、云端密码群的级别和设备端密码群的级别三者一致。

因此, 云端服务器在提取出密码, 并且对用户级别进行标记后, 那么, 待使用共享设备可以根据与用户提供的密码匹配的密码所在的设备端密码群的级别, 可以确定用户级别。

所以，当从所述设备端密码库已产生的设备端密码群中查找到与所述密码相同的密码，验证单元 403 具体用于：

利用查找到的密码和所述预设密码生成规则确定所述用户的用户级别和需求信息，完成对所述密码的同步验证。

需要说明的是，有效密码保留区的密码被使用时，不对正常级别的密码轮换产生影响，有效密码保留区中的密码直到被使用时才会消失。

当完成对密码的同步验证之后，可将级别高于用户级别的未使用的设备端密码群放到所述有效密码保留区，并删除所有级别低于所述用户级别的设备端密码群。

其中，云端密码库中的云端密码群和设备端密码库中的设备端密码群是根据预设规则逐渐产生的，并以设定规则逐渐消除低等级的密码群，以保证云端密码库的云端密码群和设备端密码库中的设备端密码群在一定数量范围内，且不重复。

云端密码群可以在提供给用户密码或用户完成一次支付行为后，增加一个或多个云端密码群，也可以通过日期，一定天数增加一定数据的云端密码群，或是根据用户使用的频繁程度，确定密码产生的数量，无效云端密码群的去除可采用以下方式：设定云端密码群有效期，超期后自动删除；在用户完成自助服务后，并反馈完成后，对所使用的云端密码群进行删除；也可以采用多种方式混合判断。

设备端密码群是否需要增加，以增加的数量以用户使用的次数、使用的时间间隔、现有有效设备端密码群数量、共享设备的工作特点、用户输入的密码等级等中的一种或多种混合方式进行确定，无效密码的消除以用户使用过自动删除为准。

经过一段使用时间后，当共享设备已获取但未用的密码增加时，有效密码保留区中的容量会越来越大，当增加到一定数量后以一定方式进行消除，以共享设备的工作特点，用户使用此次，有效密码保留区中的密码等级综合判断。

因此，共享设备还包括：

放置单元，用于当完成对所述密码的同步验证之后，将级别高于所述用户级别的未使用的设备端密码群放到所述有效密码保留区；

第一删除单元，用于删除所有级别低于所述用户级别的设备端密码群。

为进一步优化上述实施例，共享设备还包括：

第二删除单元，用于在确定所述用户的需求信息，完成对所述密码的同步验证之后，将验证成功的所述密码进行删除。

本申请还提供了一种共享设备的密码验证系统，该系统包括上述所述的云端服务器和至少一个上述所述的共享设备，其中，系统的工作原理请参见云端服务器和共享设备对应

部分，此处不再赘述。

需要说明的是，共享设备、云端服务器和密码验证系统中各组成部分的具体工作原理请参见方法实施例对应部分，此处不再赘述。

最后，还需要说明的是，在本文中，诸如第一和第二等之类的关系术语仅仅用来将一个实体或者操作与另一个实体或操作区分开来，而不一定要求或者暗示这些实体或操作之间存在任何这种实际的关系或者顺序。而且，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、物品或者设备不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、物品或者设备所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括所述要素的过程、方法、物品或者设备中还存在另外的相同要素。

本说明书中各个实施例采用递进的方式描述，每个实施例重点说明的都是与其他实施例的不同之处，各个实施例之间相同相似部分互相参见即可。

对所公开的实施例的上述说明，使本领域专业技术人员能够实现或使用本申请。对这些实施例的多种修改对本领域的专业技术人员来说将是显而易见的，本文中所定义的一般原理可以在不脱离本申请的精神或范围的情况下，在其它实施例中实现。因此，本申请将不会被限制于本文所示的这些实施例，而是要符合与本文所公开的原理和新颖特点相一致的最宽的范围。

权利要求

1、一种共享设备的密码验证方法，其特征在于，应用于云端服务器，所述云端服务器具有多个云端密码库，每一个云端密码库对应一个共享设备，所述共享设备的密码验证方法包括：

获取用户输入的待使用共享设备的设备身份，根据所述设备身份确定对应的云端密码库；

获取所述用户输入的用户信息以及对所述待使用共享设备的需求信息；

从所述云端密码库中选取一个云端密码群，并将所述云端密码群和所述用户信息以对应关系的形式进行记录；

从所述云端密码群中提取出与所述需求信息对应的密码，其中，所述密码为预先对所述需求信息采用预设密码生成规则得到的密码；

将所述密码反馈给所述用户，以使所述用户在使用所述待使用共享设备时，由所述待使用共享设备利用所述密码，从自身的设备端密码库查找是否存储有与所述密码相同的密码，如果是，则利用查找到的密码和所述预设密码生成规则确定所述用户的所述需求信息，完成对所述密码的同步验证。

2、根据权利要求 1 所述的共享设备的密码验证方法，其特征在于，所述云端密码库包括多个云端密码群，每一个云端密码群对应一位用户，每一个云端密码群为按照预设密码生成规则针对共享设备在不同工作情况的排列组合下产生的所有密码的集合。

3、根据权利要求 1 所述的共享设备的密码验证方法，其特征在于，所述设备端密码库包括多个设备端密码群，每一个设备端密码群对应一位用户，每一个共享设备在设备端密码库存储的所有密码和与该共享设备相对应的云端密码库中的密码，均是对用户的需求信息采用相同的预设密码生成规则生成。

4、根据权利要求 1 所述的共享设备的密码验证方法，其特征在于，当所述云端服务器在所述用户完成付费后，提供密码给所述用户时，从所述云端密码群中提取出与所述需求信息对应的密码，具体包括：

从所述云端密码群中提取出与所述需求信息对应的需要所述用户支付的费用；

当检测到所述用户支付完所述费用后，从所述云端密码群中提取出与所述需求信息对应的密码。

5、根据权利要求 4 所述的共享设备的密码验证方法，其特征在于，当检测到所述用户支付完所述费用后，从所述云端密码群中提取出与所述需求信息对应的密码，具体包括：

当检测到所述用户支付完所述费用后，从所述云端密码群中提取出与所述需求信息对应的密码，并标记用户级别，其中，当多个用户需要支付费用时，所述用户级别根据用户完成支付的先后顺序确定，用户完成支付的时间越靠前，相对应的用户级别越高；

将所述密码反馈给所述用户，以使所述用户在使用所述待使用共享设备时，由所述待使用共享设备利用所述密码，从自身的设备端密码库查找是否存储有与所述密码相同的密码，如果是，则利用查找到的密码确定所述用户的所述需求信息，完成对所述密码的同步验证，具体包括：

将所述密码反馈给所述用户，以使所述用户在使用所述待使用共享设备时，由所述待使用共享设备利用所述密码，从自身的设备端密码库查找是否存储有与所述密码相同的密码，如果是，则确定所述用户的用户级别和需求信息，完成对所述密码的同步验证。

6、根据权利要求 1 所述的共享设备的密码验证方法，其特征在于，所述云端密码库中所有的云端密码群和所述设备端密码库中所有的设备端密码群采用相同的密码分类分级方案。

7、一种共享设备的密码验证方法，其特征在于，应用于待使用共享设备，所述共享设备的密码验证方法包括：

获取用户在云端密码库获取的密码，所述密码为预先对需求信息采用预设密码生成规则得到的密码，所述需求信息为所述用户对所述待使用共享设备的需求信息；

利用所述密码从自身的设备端密码库查找是否存储有与所述密码相同的密码；

如果是，则利用查找到的密码和所述预设密码生成规则确定所述用户的需求信息，完成对所述密码的同步验证。

8、根据权利要求 7 所述的共享设备的密码验证方法，其特征在于，所述云端密码库包括多个云端密码群，每一个云端密码群对应一位用户，每一个云端密码群为按照预设密码生成规则针对共享设备在不同工作情况的排列组合下产生的所有密码的集合。

9、根据权利要求 7 所述的共享设备的密码验证方法，其特征在于，所述设备端密码库包括多个设备端密码群，每一个设备端密码群对应一位用户，每一个共享设备在设备端密码库存储的所有密码和与该共享设备相对应的云端密码库中的密码，均是对用户的需求信息采用相同的预设密码生成规则生成。

10、根据权利要求 7 所述的共享设备的密码验证方法，其特征在于，所述利用所述密码从自身的设备端密码库查找是否存储有与所述密码相同的密码，具体包括：

利用所述密码从自身的设备端密码库的有效密码保留区放置的设备端密码群中，查找是否存储有与所述密码相同的密码，其中，所述有效密码保留区用于保留所述待使用共享

设备已获取但未使用的密码。

11、根据权利要求 7 所述的共享设备的密码验证方法，其特征在于，所述利用所述密码从自身的设备端密码库查找是否存储有与所述密码相同的密码，具体包括：

当从自身的设备端密码库的有效密码保留区未查找到与所述密码相同的密码时，则从所述设备端密码库已产生的设备端密码群中，查找是否存储有与所述密码相同的密码。

12、根据权利要求 7 所述的共享设备的密码验证方法，其特征在于，当从所述设备端密码库已产生的设备端密码群中查找到与所述密码相同的密码，且云端密码群的级别、设备端密码群的级别和用户级别三者一致时，所述利用查找到的密码和所述预设密码生成规则确定所述用户的需求信息，完成对所述密码的同步验证，具体包括：

利用查找到的密码和所述预设密码生成规则确定所述用户的用户级别和需求信息，完成对所述密码的同步验证。

13、根据权利要求 12 所述的共享设备的密码验证方法，其特征在于，当完成对所述密码的同步验证之后，还包括：

将级别高于所述用户级别的未使用的设备端密码群放到所述有效密码保留区；

删除所有级别低于所述用户级别的设备端密码群。

14、根据权利要求 7 所述的共享设备的密码验证方法，其特征在于，在确定所述用户的需求信息，完成对所述密码的同步验证之后，还包括：

将验证成功的所述密码进行删除。

15、根据权利要求 7 所述的共享设备的密码验证方法，其特征在于，还包括：

当从所述设备端密码库未查找到与所述密码相同的密码时，输出提示信息，所述提示信息用于提示用户重新输入密码。

16、一种云端服务器，其特征在于，所述云端服务器具有多个云端密码库，每一个云端密码库对应一个共享设备，所述云端服务器包括：

第一获取单元，用于获取用户输入的待使用共享设备的设备身份，根据所述设备身份确定对应的云端密码库；

第二获取单元，用于获取所述用户输入的用户信息以及对所述待使用共享设备的需求信息；

选取单元，用于从所述云端密码库中选取一个云端密码群，并将所述云端密码群和所述用户信息以对应关系的形式进行记录；

提取单元，用于从所述云端密码群中提取出与所述需求信息对应的密码，其中，所述密码为预先对所述需求信息采用预设密码生成规则得到的密码；

反馈单元，用于将所述密码反馈给所述用户，以使所述用户在使用所述待使用共享设备时，由所述待使用共享设备利用所述密码，从自身的设备端密码库查找是否存储有与所述密码相同的密码，如果是，则利用查找到的密码和所述预设密码生成规则确定所述用户的所述需求信息，完成对所述密码的同步验证。

17、根据权利要求 16 所述的云端服务器，其特征在于，所述云端密码库包括多个云端密码群，每一个云端密码群对应一位用户，每一个云端密码群为按照预设密码生成规则针对共享设备在不同工作情况的排列组合下产生的所有密码的集合。

18、根据权利要求 16 所述的云端服务器，其特征在于，所述设备端密码库包括多个设备端密码群，每一个设备端密码群对应一位用户，每一个共享设备在设备端密码库存储的所有密码和与该共享设备相对应的云端密码库中的密码，均是对用户的需求信息采用相同的预设密码生成规则生成。

19、根据权利要求 16 所述的云端服务器，其特征在于，当所述云端服务器在所述用户完成付费后，提供密码给所述用户时，所述提取单元包括：

第一提取子单元，用于从所述云端密码群中提取出与所述需求信息对应的需要所述用户支付的费用；

第二提取子单元，用于当检测到所述用户支付完所述费用后，从所述云端密码群提取出与所述需求信息对应的密码。

20、根据权利要求 19 所述的云端服务器，其特征在于，所述第二提取子单元具体用于：

当检测到所述用户支付完所述费用后，从所述云端密码群中提取出与所述需求信息对应的密码，并标记用户级别，其中，当多个用户需要支付费用时，所述用户级别根据用户完成支付的先后顺序确定，用户完成支付的时间越靠前，相对应的用户级别越高；

所述反馈单元具体用于：

将所述密码反馈给所述用户，以使所述用户在使用所述待使用共享设备时，由所述待使用共享设备利用所述密码，从自身的设备端密码库查找是否存储有与所述密码相同的密码，如果是，则确定所述用户的用户级别和需求信息，完成对所述密码的同步验证。

21、根据权利要求 16 所述的云端服务器，其特征在于，所述云端密码库中所有的云端密码群和所述设备端密码库中所有的设备端密码群采用相同的密码分类分级方案。

22、一种共享设备，其特征在于，包括：

第三获取单元，用于获取用户在云端密码库获取的密码，所述密码为预先对需求信息采用预设密码生成规则得到的密码，所述需求信息为所述用户对所述待使用共享设备的需

求信息；

查找单元，用于利用所述密码从自身的设备端密码库查找是否存储有与所述密码相同的密码；

验证单元，用于利用查找到的密码和所述预设密码生成规则确定所述用户的需求信息，完成对所述密码的同步验证。

23、根据权利要求 22 所述的共享设备，其特征在于，所述云端密码库包括多个云端密码群，每一个云端密码群对应一位用户，每一个云端密码群为按照预设密码生成规则针对共享设备在不同工作情况的排列组合下产生的所有密码的集合。

24、根据权利要求 22 所述的共享设备，其特征在于，所述设备端密码库包括多个设备端密码群，每一个设备端密码群对应一位用户，每一个共享设备在设备端密码库存储的所有密码和与该共享设备相对应的云端密码库中的密码，均是对用户的需求信息采用相同的预设密码生成规则生成。

25、根据权利要求 22 所述的共享设备，其特征在于，所述查找单元具体用于：

利用所述密码从自身的设备端密码库的有效密码保留区放置的设备端密码群中，查找是否存储有与所述密码相同的密码，其中，所述有效密码保留区用于保留所述待使用共享设备已获取但未使用的密码。

26、根据权利要求 22 所述的共享设备，其特征在于，所述查找单元具体用于：

当从自身的设备端密码库的有效密码保留区未查找到与所述密码相同的密码时，则从所述设备端密码库已产生的设备端密码群中，查找是否存储有与所述密码相同的密码。

27、根据权利要求 22 所述的共享设备，其特征在于，当从所述设备端密码库已产生的设备端密码群中查找到与所述密码相同的密码，且云端密码群的级别、设备端密码群的级别和用户级别三者一致时，所述验证单元具体用于：

利用查找到的密码和所述预设密码生成规则确定所述用户的用户级别和需求信息，完成对所述密码的同步验证。

28、根据权利要求 27 所述的共享设备，其特征在于，还包括：

放置单元，用于当完成对所述密码的同步验证之后，将级别高于所述用户级别的未使用的设备端密码群放到所述有效密码保留区；

第一删除单元，用于删除所有级别低于所述用户级别的设备端密码群。

29、根据权利要求 22 所述的共享设备，其特征在于，还包括：

第二删除单元，用于在确定所述用户的需求信息，完成对所述密码的同步验证之后，将验证成功的所述密码进行删除。

30、根据权利要求 22 所述的共享设备，其特征在于，还包括：

输出单元，用于当从所述设备端密码库未查找到与所述密码相同的密码时，输出提示信息，所述提示信息用于提示用户重新输入密码。

31、一种共享设备的密码验证系统，其特征在于，包括权利要求 16~21 任意一项所述的云端服务器和至少一个权利要求 22~30 所述的共享设备。

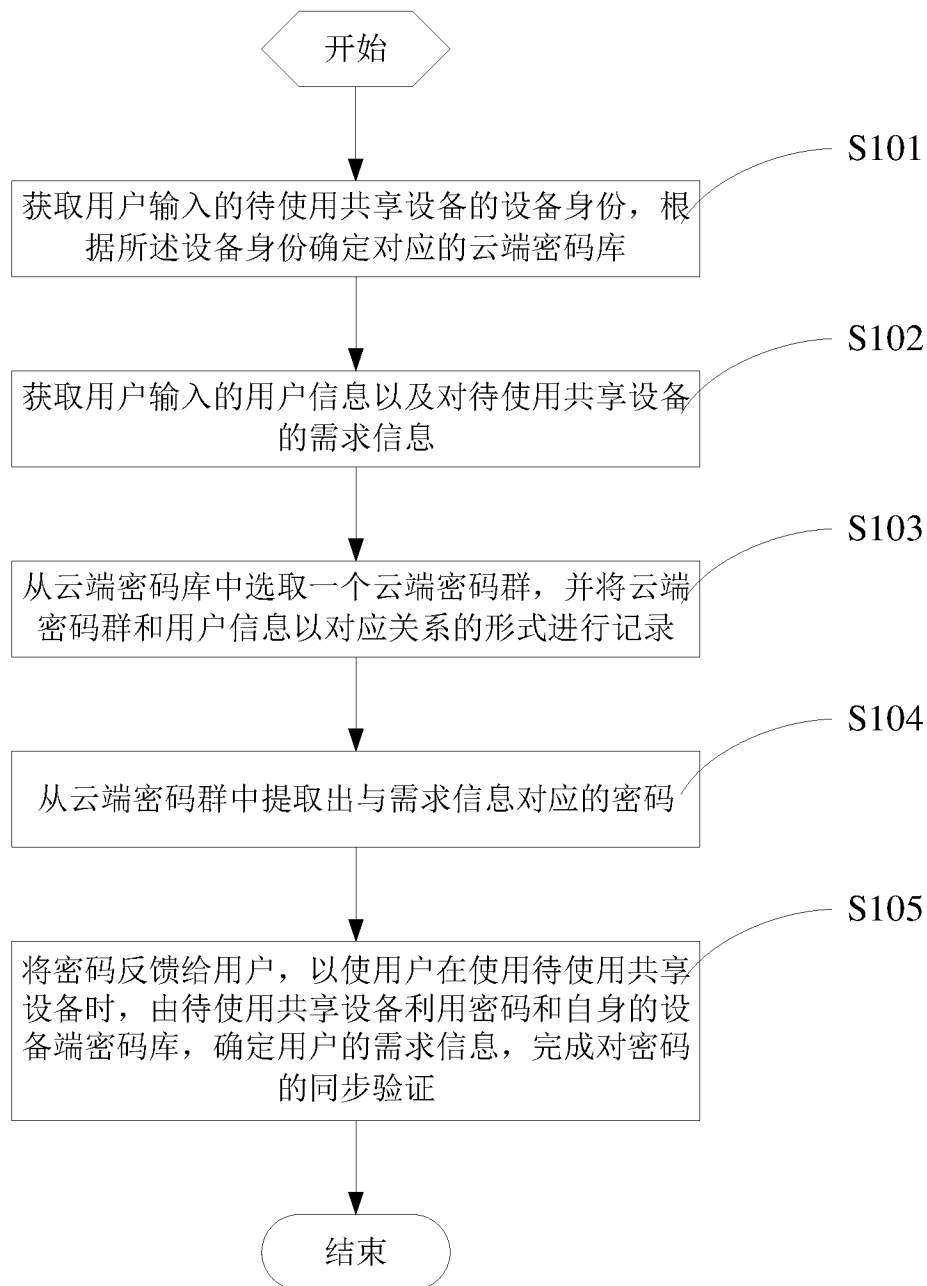


图 1

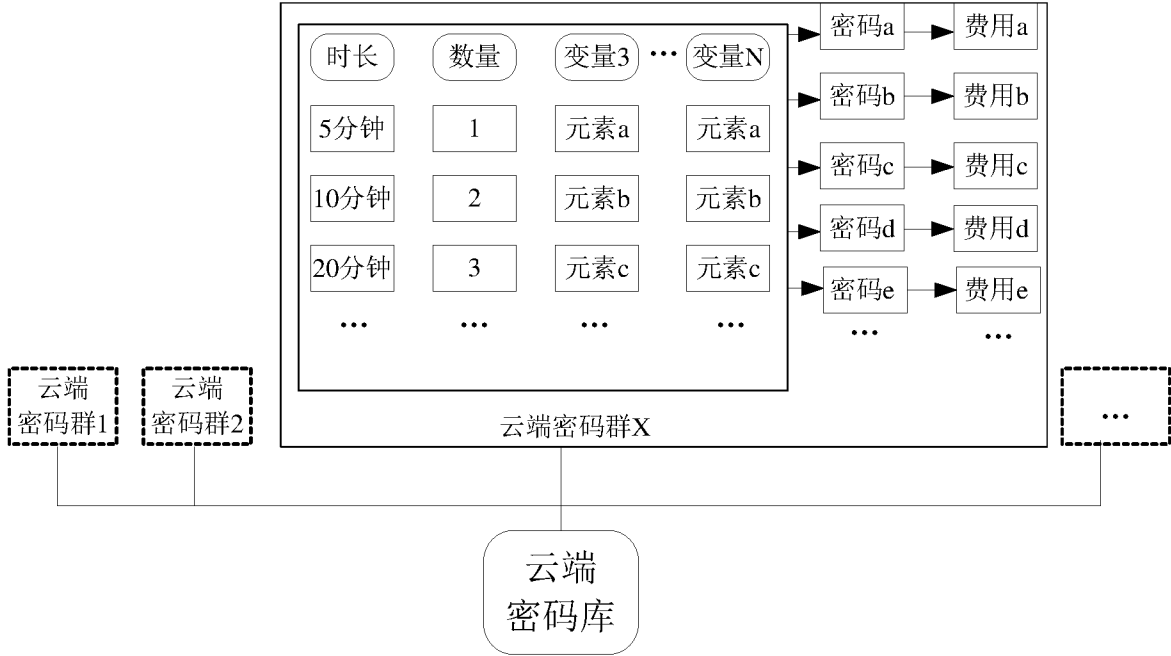


图 2

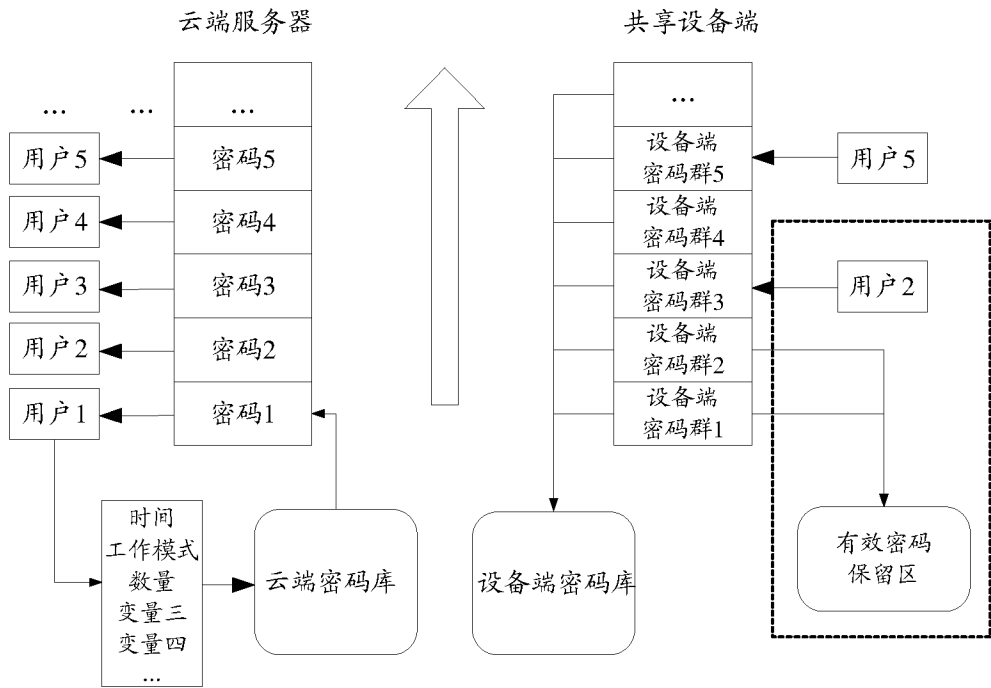


图 3

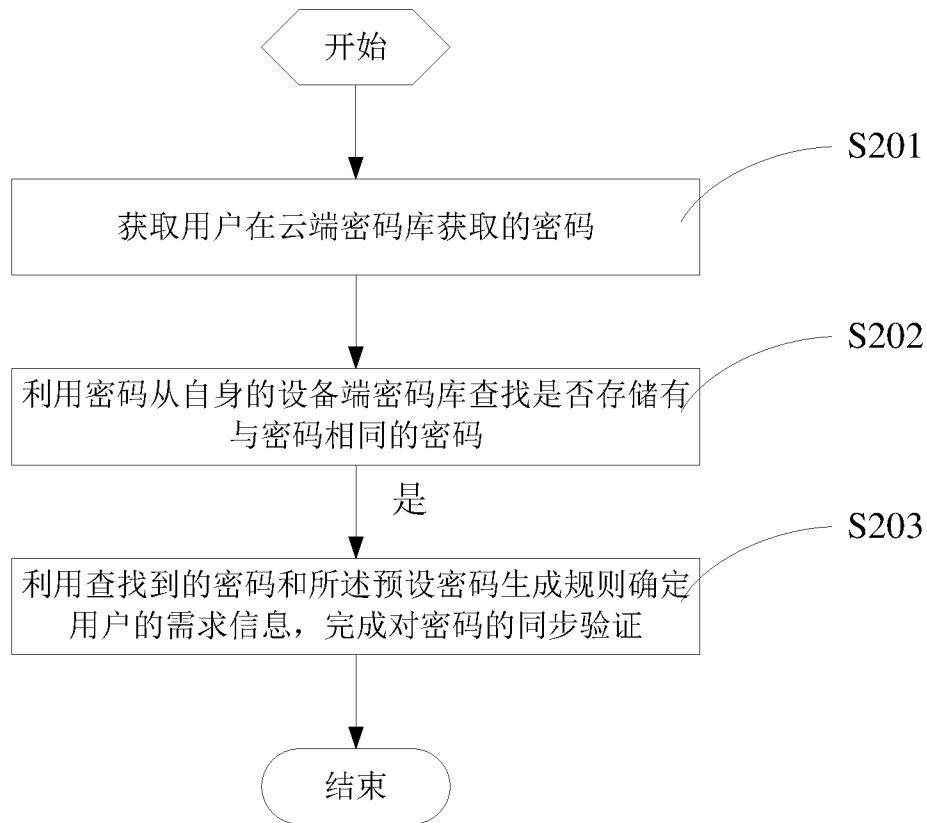


图 4

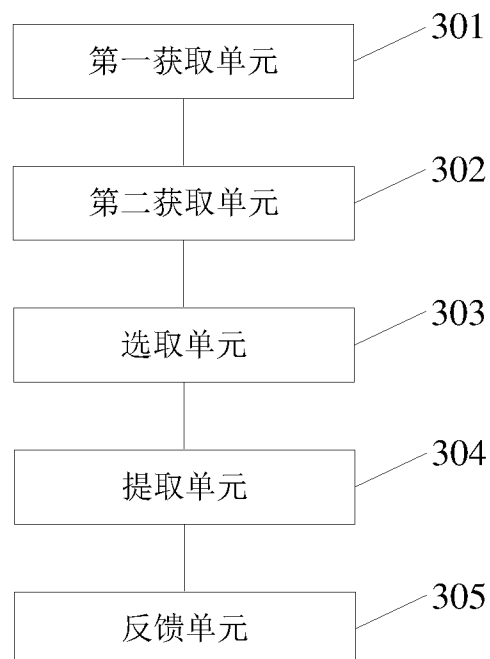


图 5

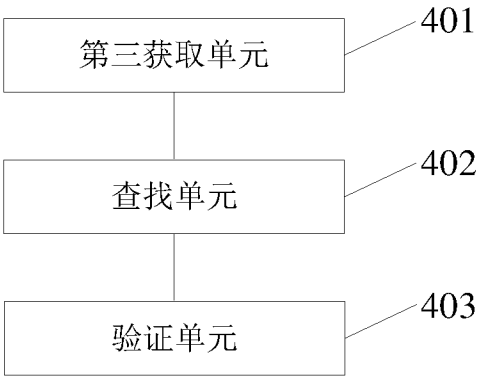


图 6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2018/090666

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/08 (2006.01) i; G07C 9/00 (2006.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L; G07C; G07F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNPAT; CNKI; WPI; EPODOC: 共享, 公共, 租, 单车, 自行车, 车, 锁, 密码, 密钥, 口令, 认证, 验证, 用户, 终端, 手机, 设备, 云, 服务器, 后台, shar+, rent+, bicycle, bike, lock, unlock, key, password, verif+, authenticat+, user, mobile, cloud, server

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 107483581 A (GREE ELECTRIC APPLIANCES INC. ZHUHAI) 15 December 2017 (15.12.2017), description, paragraphs [0087]-[0234]	1-31
X	CN 106652232 A (BEIJING BAIKE LUOKE TECHNOLOGY CO., LTD.) 10 May 2017 (10.05.2017), description, paragraphs [0048]-[0110]	1-31
X	CN 106780917 A (SHANGHAI GONGBAIKE INTELLIGENT TECHNOLOGY CO., LTD.) 31 May 2017 (31.05.2017), description, paragraphs [0033]-[0070]	1-31
X	CN 106600792 A (BEIJING BAIKE LUOKE TECHNOLOGY CO., LTD.) 26 April 2017 (26.04.2017), description, paragraphs [0049]-[0105]	1-31
A	US 2011161141 A1 (8D TECHNOLOGIES INC.) 30 June 2011 (30.06.2011), entire document	1-31

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:

“A” document defining the general state of the art which is not considered to be of particular relevance

“E” earlier application or patent but published on or after the international filing date

“L” document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

“O” document referring to an oral disclosure, use, exhibition or other means

“P” document published prior to the international filing date but later than the priority date claimed

“T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

“X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

“Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

“&” document member of the same patent family

Date of the actual completion of the international search
19 July 2018

Date of mailing of the international search report
30 July 2018

Name and mailing address of the ISA
State Intellectual Property Office of the P. R. China
No. 6, Xitucheng Road, Jimenqiao
Haidian District, Beijing 100088, China
Facsimile No. (86-10) 62019451

Authorized officer
CHEN, Xiyuan
Telephone No. (86-10) 53961594

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2018/090666

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 107483581 A	15 December 2017	None	
CN 106652232 A	10 May 2017	None	
CN 106780917 A	31 May 2017	CN 107341872 A	10 November 2017
CN 106600792 A	26 April 2017	None	
US 2011161141 A1	30 June 2011	WO 2009115925 A2	24 September 2009
		AU 2015207874 A1	20 August 2015
		US 2009240575 A1	24 September 2009
		AU 2017204273 A1	13 July 2017
		EP 2289054 A2	02 March 2011
		AU 2009227682 A1	24 September 2009
		CA 2718702 A1	24 September 2009

国际检索报告

国际申请号

PCT/CN2018/090666

A. 主题的分类

H04L 29/08(2006.01)i; G07C 9/00(2006.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

H04L; G07C; G07F

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称, 和使用的检索词(如使用))

CNPAT;CNKI;WPI;EPODOC;共享, 公共, 租, 单车, 自行车, 车, 锁, 密码, 密钥, 口令, 认证, 验证, 用户, 终端, 手机, 设备, 云, 服务器, 后台, shar+, rent+, bicycle, bike, lock, unlock, key, password, verif+, authenticat+, user, mobile, cloud, server

C. 相关文件

类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求
PX	CN 107483581 A (珠海格力电器股份有限公司) 2017年 12月 15日 (2017 - 12 - 15) 说明书第[0087]-[0234]段	1-31
X	CN 106652232 A (北京拜克洛克科技有限公司) 2017年 5月 10日 (2017 - 05 - 10) 说明书第[0048]-[0110]段	1-31
X	CN 106780917 A (上海共佰克智能科技有限公司) 2017年 5月 31日 (2017 - 05 - 31) 说明书第[0033]-[0070]段	1-31
X	CN 106600792 A (北京拜克洛克科技有限公司) 2017年 4月 26日 (2017 - 04 - 26) 说明书第[0049]-[0105]段	1-31
A	US 2011161141 A1 (8D TECHNOLOGIES INC.) 2011年 6月 30日 (2011 - 06 - 30) 全文	1-31

☐ 其余文件在C栏的续页中列出。☒ 见同族专利附件。

* 引用文件的具体类型:

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件(如具体说明的)

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期

2018年 7月 19日

国际检索报告邮寄日期

2018年 7月 30日

ISA/CN的名称和邮寄地址

中华人民共和国国家知识产权局(ISA/CN)
中国北京市海淀区蓟门桥西土城路6号 100088

传真号 (86-10)62019451

受权官员

陈希元

电话号码 86-(10)-53961594

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2018/090666

检索报告引用的专利文件			公布日 (年/月/日)	同族专利			公布日 (年/月/日)
CN	107483581	A	2017年 12月 15日	无			
CN	106652232	A	2017年 5月 10日	无			
CN	106780917	A	2017年 5月 31日	CN	107341872	A	2017年 11月 10日
CN	106600792	A	2017年 4月 26日	无			
US	2011161141	A1	2011年 6月 30日	WO	2009115925	A2	2009年 9月 24日
				AU	2015207874	A1	2015年 8月 20日
				US	2009240575	A1	2009年 9月 24日
				AU	2017204273	A1	2017年 7月 13日
				EP	2289054	A2	2011年 3月 2日
				AU	2009227682	A1	2009年 9月 24日
				CA	2718702	A1	2009年 9月 24日