



(12)发明专利申请

(10)申请公布号 CN 111369718 A

(43)申请公布日 2020.07.03

(21)申请号 202010182987.9

(22)申请日 2020.03.16

(71)申请人 杭州涂鸦信息技术有限公司
地址 310013 浙江省杭州市西湖区浙商财
富中心3幢701室

(72)发明人 黄煜静

(74)专利代理机构 北京崇智专利代理事务所
(普通合伙) 11605

代理人 何海英

(51)Int.Cl.

G07C 9/00(2020.01)

H04L 29/08(2006.01)

H04M 1/725(2006.01)

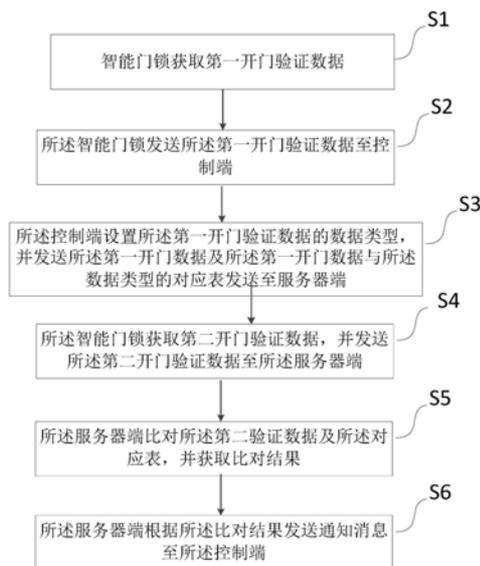
权利要求书2页 说明书5页 附图3页

(54)发明名称

一种智能门锁劫持功能标记与通知的方法及系统

(57)摘要

本申请公开了一种智能门锁劫持功能标记与通知的方法,包括:智能门锁获取第一开门验证数据;所述智能门锁发送所述第一开门验证数据至控制端;所述控制端设置所述第一开门验证数据的数据类型,并发送所述第一开门数据及所述第一开门数据与所述数据类型对应表发送至服务器端;所述智能门锁获取第二开门验证数据,并发送所述第二开门验证数据至所述服务器端;所述服务器端比所述第一验证数据及所述对应表,并获取比对结果;所述服务器端根据所述比对结果发送通知消息至所述控制端。本申请改变传统的由硬件标记劫持的方式,转为由智能门锁控制面板控制,增加或删除劫持标记,云端来判断劫持标记并发起告警通知。



1. 一种智能门锁劫持功能标记与通知的方法,其特征在于,包括:
智能门锁获取第一开门验证数据;
所述智能门锁发送所述第一开门验证数据至控制端;
所述控制端设置所述第一开门验证数据的数据类型,并发送所述第一开门数据及所述第一开门数据与所述数据类型对应表发送至服务器端;
所述智能门锁获取第二开门验证数据,并发送所述第二开门验证数据至所述服务器端;
所述服务器端比对所述第二验证数据及所述对应表,并获取比对结果;
所述服务器端根据所述比对结果发送通知消息至所述控制端。
2. 根据权利要求1所述的智能门锁劫持功能标记与通知的方法,其特征在于,所述数据类型包括:正常类型及劫持类型。
3. 根据权利要求2所述的智能门锁劫持功能标记与通知的方法,其特征在于,所述服务器端根据所述比对结果发送通知消息至所述控制端包括:
当所述第二验证数据为正常类型时,不发送所述通知消息至所述控制端;
当所述第二验证数据为劫持类型时,发送劫持消息至所述控制端。
4. 根据权利要求3所述的智能门锁劫持功能标记与通知的方法,其特征在于,智能门锁劫持功能标记与通知的方法还包括:
所述控制端修改或删除所述对应表,并发送修改或删除结果至所述服务器端;
所述服务器端根据所述修改或删除结果删除所述对应表。
5. 根据权利要求4所述的智能门锁劫持功能标记与通知的方法,其特征在于,所述第一开门验证数据包括验证数据本体及数据ID,智能门锁劫持功能标记与通知的方法还包括:
所述智能门锁发送所述验证数据本体至所述服务器端;
所述智能门锁发送所述数据ID至控制端;
所述控制端设置所述数据ID的数据类型,并发送所述数据ID与所述数据类型的第一对应表发送至服务器端;
所述服务器端生成所述数据本体,所述数据ID及所述数据类型之间的第二对应表;
所述智能门锁获取第二开门验证数据,并发送所述第二开门验证数据至所述服务器端;
所述服务器端比对所述第二验证数据及所述第二对应表,并获取比对结果;
所述服务器端根据所述比对结果发送通知消息至所述控制端。
6. 根据权利要求5所述的智能门锁劫持功能标记与通知的方法,其特征在于,所述控制端为手机app。
7. 一种智能门锁劫持功能标记与通知的系统,其特征在于,包括:
获取模块,用于智能门锁获取第一开门验证数据及第二开门验证数据;
发送模块,用于所述智能门锁发送所述第一开门验证数据至控制端及发送所述第二开门验证数据至所述服务器端;
设置模块,用于所述控制端设置所述第一开门验证数据的数据类型,并发送所述第一开门数据及所述第一开门数据与所述数据类型对应表发送至服务器端;
比对模块,用于所述服务器端比对所述第二验证数据及所述对应表,并获取比对结果;

通知模块,用于所述服务器端根据所述比对结果发送通知消息至所述控制端。

8.一种计算机设备,包括存储器、处理器和存储在所述存储器内并能由所述处理器运行的计算机程序,其特征在于,所述处理器执行所述计算机程序时实现如权利要求1-6中任一项所述的方法。

9.一种计算机可读存储介质,非易失性可读存储介质,其内存储有计算机程序,其特征在于,所述计算机程序在由处理器执行时实现如权利要求1-6中任一项所述的方法。

10.一种计算机程序产品,包括计算机可读代码,其特征在于,当所述计算机可读代码由计算机设备执行时,导致所述计算机设备执行权利要求1-6中任一项所述的方法。

一种智能门锁劫持功能标记与通知的方法及系统

技术领域

[0001] 本申请涉及物联网领域,具体而言,涉及一种智能门锁劫持功能标记与通知的方法。

背景技术

[0002] 现有的智能门锁在常用解锁方式(如指纹开门、密码开门、门卡开门等)的添加通常为在设备端开始发起(这里我们以密码为例),先验证管理员身份,再对普通密码设置录入,如果是带有劫持功能的门锁,则也是和普通密码的录入过程一样,需要在设备端进行录入并标记该密码为劫持密码,当使用该劫持密码开门时会有劫持告警通知。

[0003] 另外,在设备端录入标记管理不便,用户一旦添加成功后不可更改,需要在设备端删除或重新添加,操作繁琐,用户体验性很差,与此同时,用户不能够清楚的知道当前添加的劫持密码绑定在哪个成员下,不够直观,明确。

发明内容

[0004] 本申请的主要目的在于提供一种智能门锁劫持功能标记与通知的方法,包括:

[0005] 智能门锁获取第一开门验证数据;

[0006] 所述智能门锁发送所述第一开门验证数据至控制端;

[0007] 所述控制端设置所述第一开门验证数据的数据类型,并发送所述第一开门数据及所述第一开门数据与所述数据类型的对应表发送至服务器端;

[0008] 所述智能门锁获取第二开门验证数据,并发送所述第二开门验证数据至所述服务器端;

[0009] 所述服务器端比对所述第二验证数据及所述对应表,并获取比对结果;

[0010] 所述服务器端根据所述比对结果发送通知消息至所述控制端。

[0011] 可选地,所述数据类型包括:正常类型及劫持类型。

[0012] 可选地,所述服务器端根据所述比对结果发送通知消息至所述控制端包括:

[0013] 当所述第二验证数据为正常类型时,不发送所述通知消息至所述控制端;

[0014] 当所述第二验证数据为劫持类型时,发送劫持消息至所述控制端。

[0015] 可选地,智能门锁劫持功能标记与通知的方法还包括:

[0016] 所述控制端修改或删除所述对应表,并发送修改或删除结果至所述服务器端;

[0017] 所述服务器端根据所述修改或删除结果删除所述对应表。

[0018] 可选地,所述第一开门验证数据包括验证数据本体及数据ID,智能门锁劫持功能标记与通知的方法还包括:

[0019] 所述智能门锁发送所述验证数据本体至所述服务器端;

[0020] 所述智能门锁发送所述数据ID至控制端;

[0021] 所述控制端设置所述数据ID的数据类型,并发送所述数据ID与所述数据类型的第一对应表发送至服务器端;

- [0022] 所述服务器端生成所述数据本体,所述数据ID及所述数据类型之间的第二对应表;
- [0023] 所述智能门锁获取第二开门验证数据,并发送所述第二开门验证数据至所述服务器端;
- [0024] 所述服务器端比对所述第二验证数据及所述第二对应表,并获取比对结果;
- [0025] 所述服务器端根据所述比对结果发送通知消息至所述控制端。
- [0026] 可选地,所述控制端为手机app。
- [0027] 根据本申请的另一个方面,还提供了一种智能门锁劫持功能标记与通知的系统,包括:
- [0028] 获取模块,用于智能门锁获取第一开门验证数据及第二开门验证数据;
- [0029] 发送模块,用于所述智能门锁发送所述第一开门验证数据至控制端及发送所述第二开门验证数据至所述服务器端;
- [0030] 设置模块,用于所述控制端设置所述第一开门验证数据的数据类型,并发送所述第一开门数据及所述第一开门数据与所述数据类型的对应表发送至服务器端;
- [0031] 比对模块,用于所述服务器端比对所述第二验证数据及所述对应表,并获取比对结果;
- [0032] 通知模块,用于所述服务器端根据所述比对结果发送通知消息至所述控制端。
- [0033] 本申请还公开了一种计算机设备,包括存储器、处理器和存储在所述存储器内并能由所述处理器运行的计算机程序,所述处理器执行所述计算机程序时实现上述任一项所述的方法。
- [0034] 本申请还公开了一种计算机可读存储介质,非易失性可读存储介质,其内存储有计算机程序,所述计算机程序在由处理器执行时实现上述任一项所述的方法。
- [0035] 本申请还公开了一种计算机程序产品,包括计算机可读代码,当所述计算机可读代码由计算机设备执行时,导致所述计算机设备执行上述任一项所述的方法。
- [0036] 与现有技术相比,本申请具有如下有益效果:
- [0037] 改变传统的由硬件标记劫持的方式,转为由智能门锁控制面板控制,增加或删除劫持标记,云端来判断劫持标记并发起告警通知。减少了设备端的操作,用户可以随时随地对已存在的开门方式进行劫持标记添加与移除使得用户操作更为简单,提升用户体验。
- [0038] 减少固件的判断逻辑,劫持告警通知由云端来判断并发起,大大减少了设备的损耗。固件处理逻辑更加简单。只需要做普通的指纹密码的录入即可。意味着原本不支持劫持功能的普通智能门锁也可以依赖此方案直接快速支持劫持告警功能。

附图说明

- [0039] 构成本申请的一部分的附图用来提供对本申请的进一步理解,使得本申请的其它特征、目的和有益效果变得更明显。本申请的示意性实施例附图及其说明用于解释本申请,并不构成对本申请的不当限定。在附图中:
- [0040] 图1是根据本申请一个实施例的智能门锁劫持功能标记与通知的方法的流程示意图;
- [0041] 图2是根据本申请一个实施例的智能门锁劫持功能标记与通知的方法的流程示意

图；

[0042] 图3是根据本申请一个实施例的计算机设备的示意图；以及

[0043] 图4是根据本申请一个实施例的计算机可读存储介质的示意图。

具体实施方式

[0044] 为了使本技术领域的人员更好地理解本申请方案，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的实施例，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，都应当属于本申请保护的范围。

[0045] 需要说明的是，本申请的说明书和权利要求书及上述附图中的术语“第一”、“第二”等是用于区别类似的对象，而不必用于描述特定的顺序或先后次序。应该理解这样使用的数据在适当情况下可以互换，以便这里描述的本申请的实施例。此外，术语“包括”和“具有”以及他们的任何变形，意图在于覆盖不排他的包含，例如，包含了一系列步骤或单元的过程、方法、系统、产品或设备不必限于清楚地列出的那些步骤或单元，而是可包括没有清楚地列出的或对于这些过程、方法、产品或设备固有的其它步骤或单元。

[0046] 需要说明的是，在不冲突的情况下，本申请中的实施例及实施例中的特征可以相互组合。下面将参考附图并结合实施例来详细说明本申请。

[0047] 请参照图1-图2，本申请一实施例提供了一种智能门锁劫持功能标记与通知的方法，包括：

[0048] S1：智能门锁获取第一开门验证数据；

[0049] S2：所述智能门锁发送所述第一开门验证数据至控制端；

[0050] S3：所述控制端设置所述第一开门验证数据的数据类型，所述控制端发送所述第一开门数据及所述第一开门数据与所述数据类型的对应表发送至服务器端；

[0051] S4：所述智能门锁获取第二开门验证数据，并发送所述第二开门验证数据至所述服务器端；

[0052] S5：所述服务器端比对所述第二验证数据及所述对应表，在所述对应表中寻找所述第二验证数据，并获取比对结果；

[0053] S6：所述服务器端根据所述比对结果发送或者不发送通知消息至所述控制端。

[0054] 例如，用户在最初录入指纹时，分别录入了食指和中指。然后门锁将食指指纹和中指指纹发送至控制端。控制端将食指指纹设置成正常类型，将中指指纹设置成劫持类型。形成对应表之后将食指指纹、中指指纹以及该对应表发送至服务器。

[0055] 然后，用户在开门时，当其使用食指进行指纹验证时，门锁将食指指纹发送至服务器，服务器将该食指指纹与对应表中的指纹进行比对。发现食指指纹对应的是正常类型，则发送开门指令至门锁，门锁根据开门指令开锁。当用户使用中指进行指纹验证时，门锁将中指指纹发送至服务器，服务器将该中指指纹与对应表中的指纹进行比对。发现中指指纹对应的是劫持类型，则不发送开门指令至门锁，并发送劫持信息至控制端；或者发送开门指令至门锁，并发送劫持信息至控制端。

[0056] 对于固件（设备端）来说，只需要做最基本的指纹、密码、门卡的创建即可，本地固

件不需要写入劫持相关的逻辑。

[0057] 对于控制面板来说,当在指纹、密码、门卡录入时,或者对早已录入的指纹、密码、门卡进行标记,具体表现为:在开门方式成功创建后可以通过设备端拿到当前创建的开门方式的硬件编号,当在面板中设置为劫持后,只需将对应的硬件编号告知云端服务器并保存,除此之外,在收到云端的消息推送时,进行对应的告警数据展示。

[0058] 对于云端服务器来说,当控制面板将具体某个硬件编号设置为劫持时,需要存在服务器上,在每次触发开门时,将固件开门动作所上报的编号进行逐一比对,若开门的硬件编号同标记为劫持的硬件编号一致,则说明此次为劫持开门,同时将这条劫持的消息通过MQTT消息推送给APP,告知此次开门方式为劫持开门固件无需专门对劫持功能做逻辑处理,可以保证普通智能门锁可以快速接入劫持告警功能,无需固件重复开发。

[0059] 面板可以对任意的指纹密码门卡进行标记为劫持,并可以直观看到当前劫持在哪个家庭成员下,使得该功能展示更加清晰,可视化。便于操作,易于管理。

[0060] 本申请一实施例中,所述数据类型包括:正常类型及劫持类型。

[0061] 本申请一实施例中,所述服务器端根据所述比对结果发送通知消息至所述控制端包括:

[0062] 当所述第二验证数据为正常类型时,不发送所述通知消息至所述控制端;

[0063] 当所述第二验证数据为劫持类型时,发送劫持消息至所述控制端。

[0064] 本申请一实施例中,智能门锁劫持功能标记与通知的方法还包括:

[0065] 所述控制端修改或删除所述对应表,并发送修改或删除结果至所述服务器端;

[0066] 所述服务器端根据所述修改或删除结果删除所述对应表。

[0067] 删除也是同样的道理,对于已经标记的劫持功能的指纹、密码、门卡移除时,只需将对应编号通过接口告知云端服务器。

[0068] 本申请一实施例中,所述第一开门验证数据包括验证数据本体及数据ID,智能门锁劫持功能标记与通知的方法还包括:

[0069] 所述智能门锁发送所述验证数据本体至所述服务器端;

[0070] 所述智能门锁发送所述数据ID至控制端;

[0071] 所述控制端设置所述数据ID的数据类型,并发送所述数据ID与所述数据类型的第一对应表发送至服务器端;

[0072] 所述服务器端生成所述数据本体,所述数据ID及所述数据类型之间的第二对应表;

[0073] 所述智能门锁获取第二开门验证数据,并发送所述第二开门验证数据至所述服务器端;

[0074] 所述服务器端比对所述第二验证数据及所述第二对应表,并获取比对结果;

[0075] 所述服务器端根据所述比对结果发送通知消息至所述控制端。

[0076] 例如,数据本体指的是指纹本身,数据ID指的是该指纹本体所对应的唯一的编号。例如食指指纹编号为1,中指指纹编号为2。如此门锁只需要把编号发给控制端,控制端把编号号类型对应起来即可,不需要指纹本身的信息传输,减少了信息传输量。

[0077] 本申请一实施例中,所述控制端为手机app。

[0078] 本申请一实施例还提供了一种智能门锁劫持功能标记与通知的系统,包括:

- [0079] 获取模块,用于智能门锁获取第一开门验证数据及第二开门验证数据;
- [0080] 发送模块,用于所述智能门锁发送所述第一开门验证数据至控制端及发送所述第二开门验证数据至所述服务器端;
- [0081] 设置模块,用于所述控制端设置所述第一开门验证数据的数据类型,并发送所述第一开门数据及所述第一开门数据与所述数据类型的对应表发送至服务器端;
- [0082] 比对模块,用于所述服务器端比对所述第二验证数据及所述对应表,并获取比对结果;
- [0083] 通知模块,用于所述服务器端根据所述比对结果发送通知消息至所述控制端。
- [0084] 与现有技术相比,本申请具有如下有益效果:
- [0085] 改变传统的由硬件标记劫持的方式,转为由智能门锁控制面板控制,增加或删除劫持标记,云端来判断劫持标记并发起告警通知。减少了设备端的操作,用户可以随时随地对已存在的开门方式进行劫持标记添加与移除使得用户操作更为简单,提升用户体验。
- [0086] 减少固件的判断逻辑,劫持告警通知由云端来判断并发起,大大减少了设备的损耗。固件处理逻辑更加简单。只需要做普通的指纹密码的录入即可。意味着原本不支持劫持功能的普通智能门锁也可以依赖此方案直接快速支持劫持告警功能。
- [0087] 请参照图3,本申请还提供了一种计算机设备,包括存储器、处理器和存储在所述存储器内并能由所述处理器运行的计算机程序,所述处理器执行所述计算机程序时实现上述任一项所述的方法。
- [0088] 请参照图4,一种计算机可读存储介质,非易失性可读存储介质,其内存储有计算机程序,所述计算机程序在由处理器执行时实现上述任一项所述的方法。
- [0089] 一种计算机程序产品,包括计算机可读代码,当所述计算机可读代码由计算机设备执行时,导致所述计算机设备执行上述任一项所述的方法。
- [0090] 显然,本领域的技术人员应该明白,上述的本发明的各模块或各步骤可以用通用的计算装置来实现,它们可以集中在单个的计算装置上,或者分布在多个计算装置所组成的网络上,可选地,它们可以用计算装置可执行的程序代码来实现,从而,可以将它们存储在存储装置中由计算装置来执行,或者将它们分别制作成各个集成电路模块,或者将它们中的多个模块或步骤制作成单个集成电路模块来实现。这样,本发明不限制于任何特定的硬件和软件结合。
- [0091] 以上所述仅为本申请的优选实施例而已,并不用于限制本申请,对于本领域的技术人员来说,本申请可以有各种更改和变化。凡在本申请的精神和原则之内,所作的任何修改、等同替换、改进等,均应包含在本申请的保护范围之内。

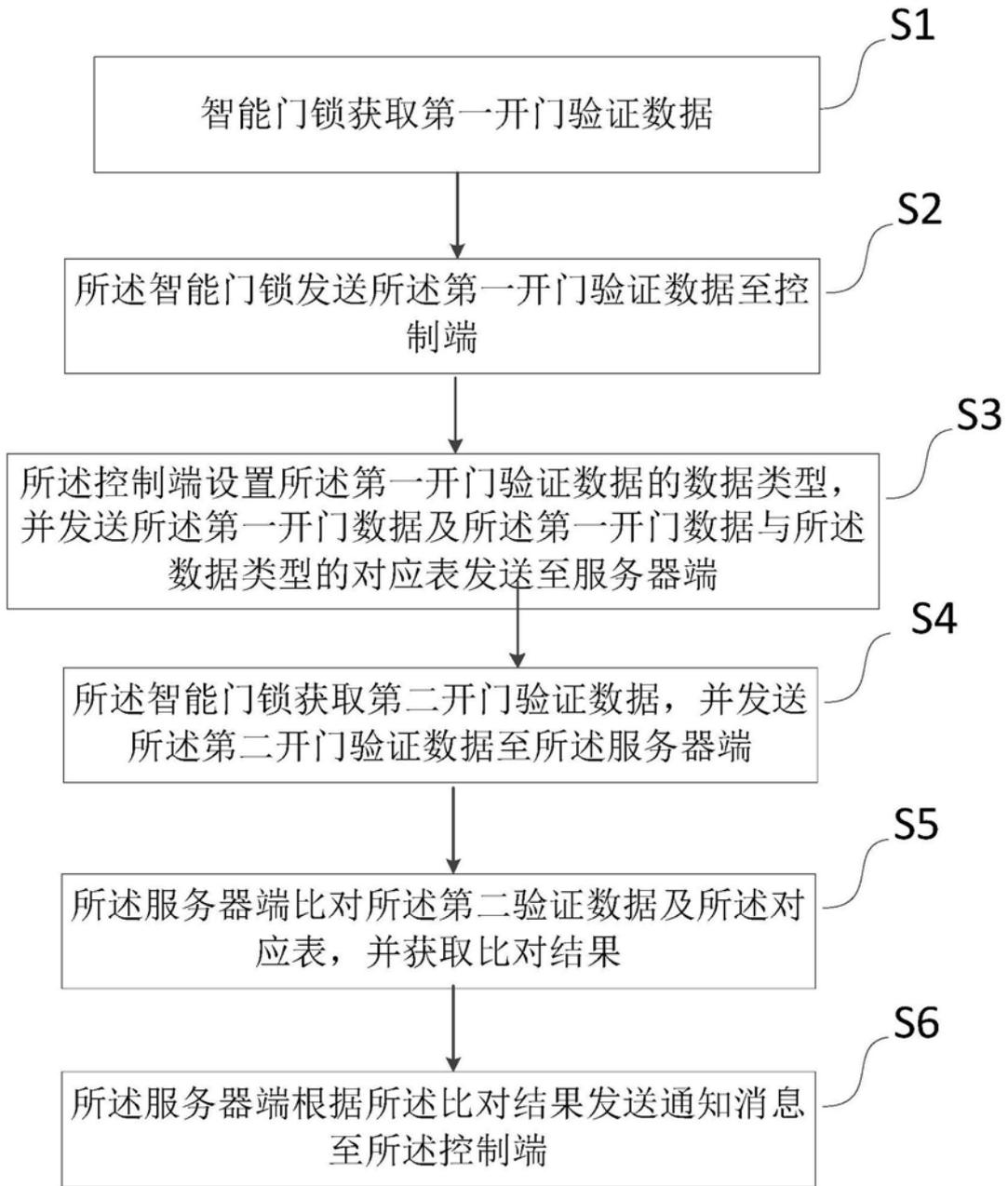


图1

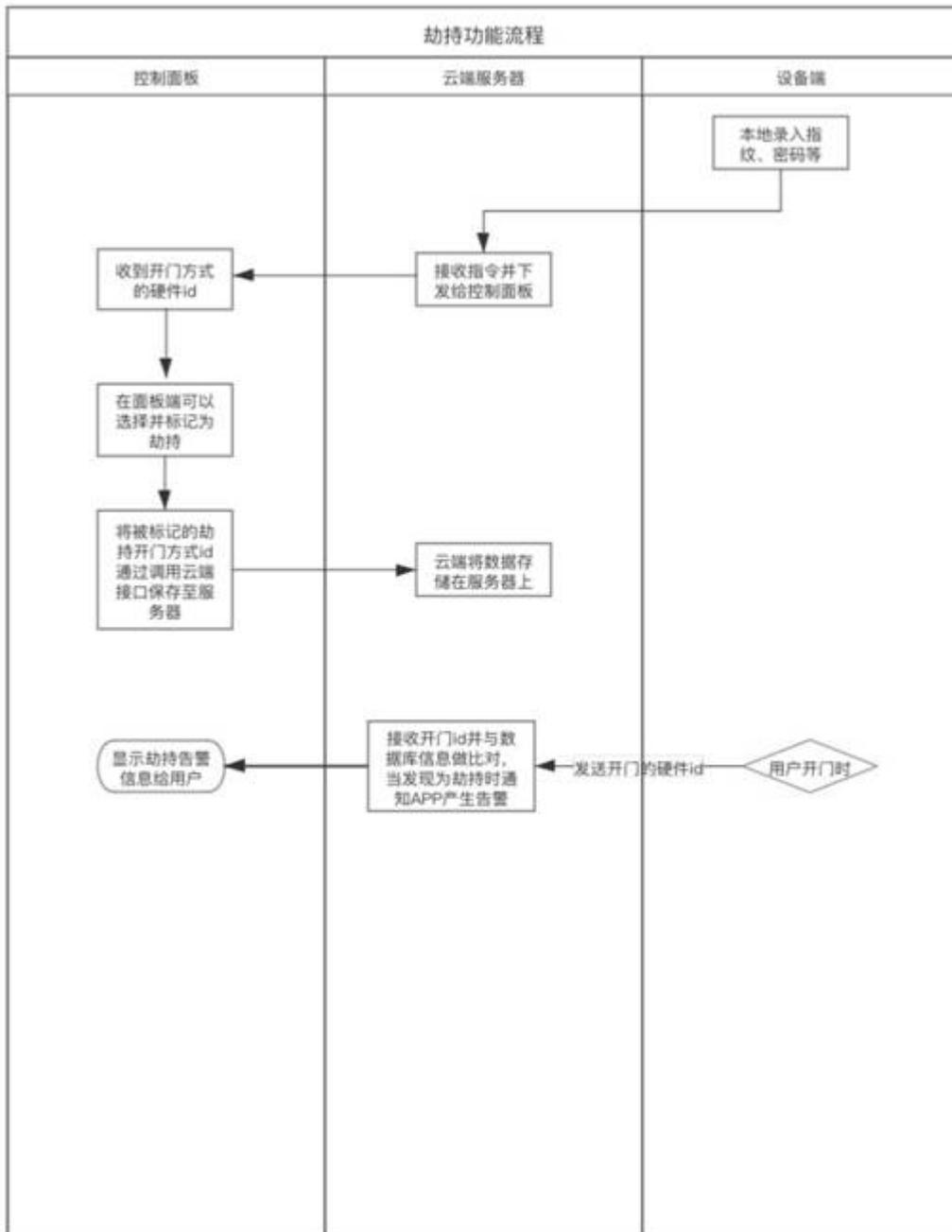


图2

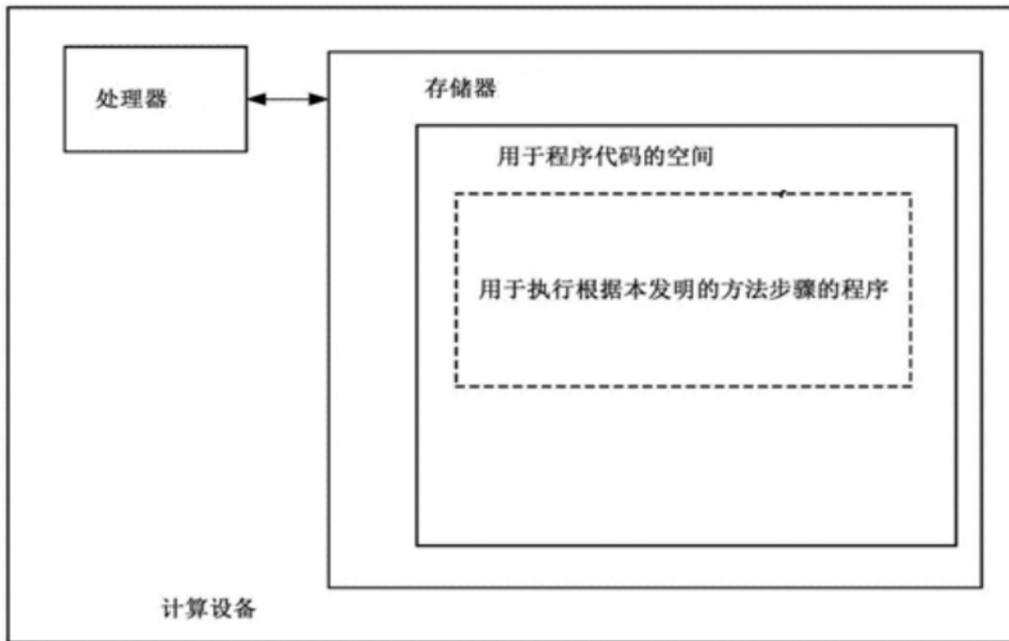


图3

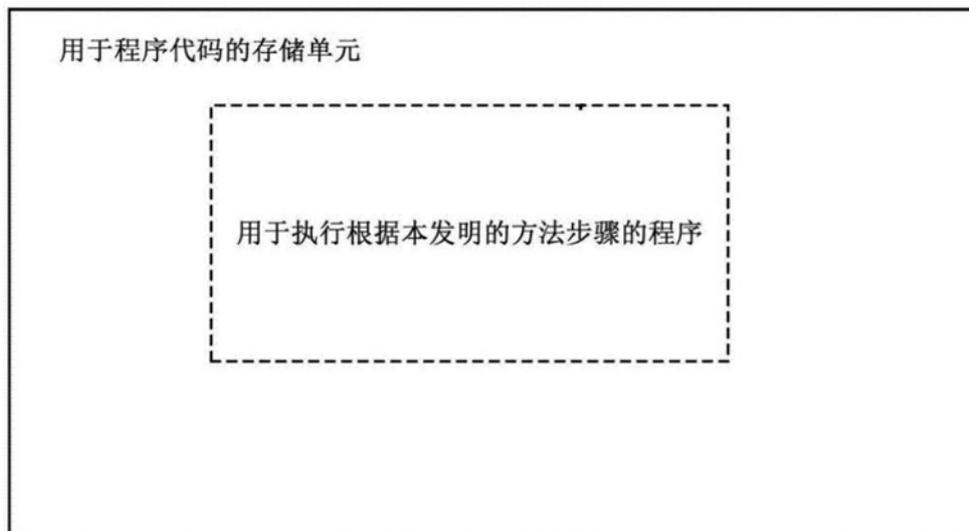


图4