

(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
2020 年 8 月 20 日 (20.08.2020)

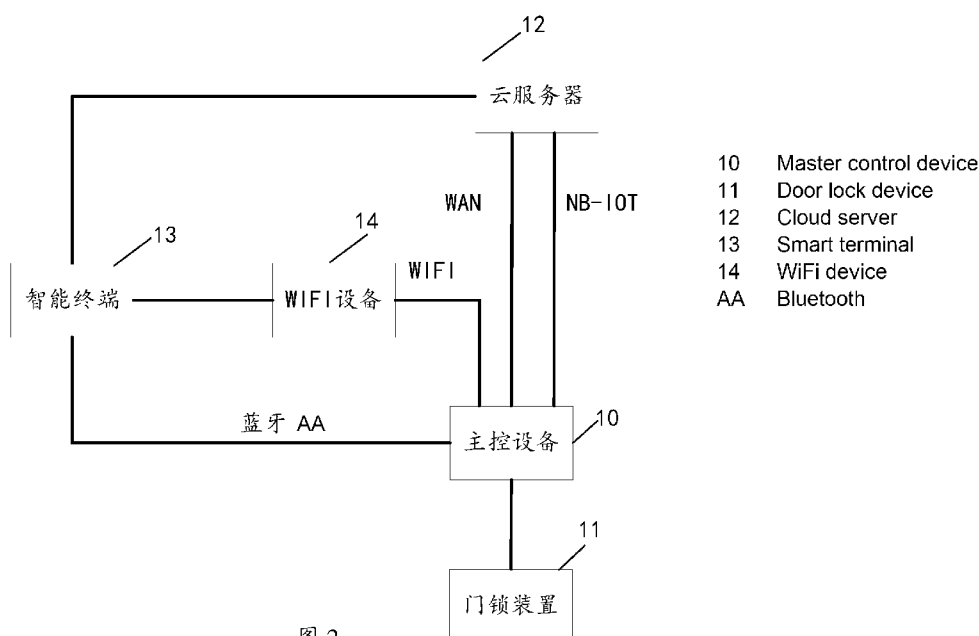


(10) 国际公布号
WO 2020/164104 A1

- (51) 国际专利分类号:
G07C 9/00 (2006.01) *H04L 29/08* (2006.01)
- (21) 国际申请号: PCT/CN2019/075210
- (22) 国际申请日: 2019 年 2 月 15 日 (15.02.2019)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (71) 申请人: 深圳市汇顶科技股份有限公司(SHENZHEN GOODIX TECHNOLOGY CO.,LTD.)
[CN/CN]; 中国广东省深圳市福田区腾飞工业大厦B座13层, Guangdong 518045 (CN)。
- (72) 发明人: 白海 (BAI, Hai); 中国广东省深圳市福田区腾飞工业大厦B座13层, Guangdong 518045 (CN)。
- (74) 代理人: 上海晨皓知识产权代理事务所(普通合伙)(SHANGHAI CHENHAO INTELLECTUAL PROPERTY LAW FIRM GENERAL PARTNERSHIP); 中国上海市黄浦区制造局路787号二幢202B室, Shanghai 200011 (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, 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,

(54) **Title:** PROCESSING CHIP, MASTER CONTROL DEVICE, AND ACCESS CONTROL SYSTEM AND UNLOCKING METHOD THEREOF

(54) 发明名称: 处理芯片、主控设备、门禁系统及其解锁方法



(57) **Abstract:** A processing chip, a master control device, and an access control system and an unlocking method thereof. The access control system comprises: a master control device (10), a door lock device (11), a cloud server (12), and at least one smart terminal (13). The master control device (10) is connected to the cloud server (12) and the door lock device (11); the smart terminal (13) is connected to the cloud server (12); in a first mode, the smart terminal (13) is configured to send an unlock request to the master device (10) by means of the cloud server (12); the master control device (10) is configured to determine, upon receiving the unlocking request,

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))。

whether unlocking is allowed according to the unlocking request, and upon determining that unlocking is allowed, control the door lock device (11) to unlock. The access control system can improve the security of the access control system.

(57) 摘要: 一种处理芯片、主控设备、门禁系统及其解锁方法, 该门禁系统包括: 主控设备(10)、门锁装置(11)、云服务器(12)以及至少一智能终端(13); 主控设备(10)连接于云服务器(12)和门锁装置(11), 智能终端(13)连接于云服务器(12); 智能终端(13)用于在处于第一模式时, 通过云服务器(12)发送解锁请求至主控设备(10); 主控设备(10)用于在接收到解锁请求时, 根据解锁请求判断是否允许解锁, 并在判定允许解锁时, 控制门锁装置(11)解锁。该门禁系统可以提高门禁系统的安全性。

处理芯片、主控设备、门禁系统及其解锁方法

技术领域

[0001] 本申请涉及门禁控制技术领域，特别涉及一种主控设备、门禁系统及其解锁方法。

背景技术

[0002] 随着人们生活进步，对家庭住宅、办公等场所进出的便捷性和安全性越来越高，很多需要经常进出的地方都安装了门禁系统。

[0003] 门禁系统的解锁方式多种多样，如 NFC（基于 NFC 的门禁卡）、指纹密码、数字密码等离线解锁，以及基于云服务器（远程解锁）、或基于近距离无线传输技术的在线解锁，大大丰富了解锁方式。其中，在基于云服务器的在线解锁中，云服务器接收智能终端的解锁请求，并根据解锁请求来确定是否允许解锁；即云服务器是远程解锁的一个重要环节，其内部存储着终端用户及门禁解锁的核心数据。

[0004] 发明人发现现有技术至少存在以下问题：云服务器作为复杂网络的中心节点，要处理的业务种类繁多且需要与众多设备交互，较容易被不法分子入侵并盗取核心数据或篡改门禁权限。

发明内容

[0005] 本申请部分实施例的目的在于提供一种处理芯片、主控设备、门禁系统及其解锁方法，可以提高门禁系统的安全性。

[0006] 本申请实施例提供了一种门禁系统，包括：主控设备、门锁装置、云服务器以及至少一智能终端；所述主控设备连接于所述云服务器和所述门锁装置，所述智能终端连接于所述云服务器；所述智能终端用于在处于第一模式时，通过所述云服务器发送解锁请求至所述主控设备；所述主控设备用于在接收到所述解锁请求时，根据所述解锁请求判断是否允许解锁，并在判定允许解锁时，控制所述门锁装置解锁。

[0007] 本申请实施例还提供了一种门禁系统的解锁方法，应用于所述门禁系统中的主控设备，所述门禁系统还包括云服务器、门锁装置以及至少一智能终端；所述智能终端用于在处于第一模式时，通过所述云服务器发送解锁请求至所述主控设备；所述解锁方法包括：当接收到所述解锁请求时，根据所述解锁请求判断是否允许解锁；当判定允许解锁时，控制所述门锁装置解锁。

[0008] 本申请实施例还提供了一种处理芯片，与至少一存储器连接，所述存储器存储有可被所述处理芯片执行的指令，所述指令被所述处理芯片执行，以使所述处理芯片能够执行上述门禁系统的解锁方法。

[0009] 本申请实施例还提供了一种主控设备，包括上述处理芯片。

[0010] 本申请实施例相对于现有技术而言，由主控设备判断是否允许解锁，由于本案中的主控设备相当于复杂网络结构中的边缘节点，相较于作为网络中心的云服务器而言（现有技术中由云服务器判断是否允许解锁），被非法入侵的难度较大，因此可以提高门禁系统的安全性。

[0011] 另外，所述云服务器还用于在监测到预设事件发生时，发送预警信号至所述主控设备；所述主控设备还用于在接收到所述预警信号时，进入预设的控制模式。本实施例中，云服务器可以主动监测预设事件，并在预设事件发生时告知主控设备，从而使得主控设备进入预设的控制模式；可以满足更多的实际应用场景的需要。

[0012] 另外，所述云服务器包含多个分布式站点；各所述分布式站点用于在监测到所述预设事件发生时，分别发送所述预警信号至所述主控设备；所述主控设备用于在接收到各所述分布式站点发送的所述预警信号时，进入预设的控制模式。本实施例中，云服务器为分布式结构，主控设备同时接收到多个分布式站点的预警信号才进入预设的控制模式，可靠性更高。

[0013] 另外，所述智能终端包括管理员终端和普通用户终端；所述普通用户终端用于在预设的紧急事件发生时，向所述管理员终端发送紧急解锁请求；其中，其中，在所述紧急事件发生时，所述普通用户终端不具备解锁权限；所述管理员终端用于对所述紧急解锁请求进行认证，并将经过认证的所述紧急解锁请求发送至所述主控设备；所述主控设备在接收到经过认证的所述紧急解锁请求后，控制所述门锁装置解锁。本实施例中，在紧急情况发生时，不具备解锁权限的普通用户终端可以通过向管理员终端发送紧急解锁请求来实现紧急解锁；可以满足更多的实际应用场景的需要。

[0014] 另外，所述门禁系统还包括连接于所述智能终端的辅助定位设备；所述智能终端还用于在处于所述第一模式时，通过所述辅助定位设备获取所述智能终端的定位信息，所述解锁请求包括所述定位信息。本实施例中，可以结合定位信息来判断是否允许解锁，可以满足更多的实际应用场景的需求。

[0015] 另外，所述门禁系统还包括连接于所述主控设备的存储设备；所述主控设备还用于在根据所述解锁请求判断是否允许解锁后，生成所述解锁请求的解锁记录，并将所述解锁记录存储至所述存储设备；其中，所述解锁记录至少包括：所述主控设备根据所述解锁请求识别出的发送所述解锁请求的用户，以及是否解锁成功。本实施例中，可以对每次解锁请求的过程进行记录。

[0016] 另外，所述门锁装置安装于可移动设备中。本实施例中，即使可移动设备被非法盗取，由于其与主控设备无法连接，从而盗窃者无法通过软件侵入方式进行解锁，在一定程度上提高了安全性。

[0017] 另外，所述智能终端还用于在处于第二模式时，基于近距离无线传输技术发送所述解锁请求至所述主控设备。本实施例提供了智能终端将解锁请求发送至主控设备的另一种途径。

[0018] 另外，在门禁系统的解锁方法中，在所述生成所述解锁请求的解锁记录，并将所述解锁记录上传至所述存储设备进行存储之前，还包括：判定所述主控设备根据所述解锁请求获取的所述用户对应的门禁权限中不包含匿名权限。本实施例中，不会对拥有匿名权限的用户的解锁请求进行记录；本实施例丰富了用户的门禁权限种类，可以满足更多的实际应用场景的需求。

附图说明

[0019] 一个或多个实施例通过与之对应的附图中的图片进行示例性说明，这些示例性说明并不构成对实施例的限定，附图中具有相同参考数字标号的元件表示为类似的元件，除非有特别申明，附图中的图不构成比例限制。

[0020] 图 1 是根据本申请第一实施例的门禁系统的一个示意图；

[0021] 图 2 是根据本申请第一实施例的门禁系统的另一个示意图；

[0022] 图 3 是根据本申请第三实施例的门禁系统的示意图；

[0023] 图 4 是根据本申请第四实施例的门禁系统的示意图；

[0024] 图 5 是根据本申请第五实施例的门禁系统的示意图；

[0025] 图 6 是根据本申请第六实施例的门禁系统的解锁方法的流程图；

[0026] 图 7 是根据本申请第六实施例中根据解锁请求判断是否允许解锁这一步骤的具体流程图；

[0027] 图 8 是根据本申请第七实施例的门禁系统的解锁方法的流程图；

[0028] 图 9 是根据本申请第八实施例中根据解锁请求判断是否允许解锁这一步骤的具体流程图；

[0029] 图 10 是根据本申请第九实施例的门禁系统的解锁方法的流程图；

[0030] 图 11 是根据本申请第十实施例的处理芯片与存储器连接的示意图。

具体实施方式

[0031] 为了使本申请的目的、技术方案及优点更加清楚明白，以下结合附图及实施例，对本申请部分实施例进行进一步详细说明。应当理解，此处所描述的具体实施例仅仅用以解释本申请，并不用于限定本申请。

[0032] 本申请第一实施例涉及一种门禁系统，如图 1 所述，门禁系统包括：主控设备 10、门锁装置 11、云服务器 12 以及至少一智能终端 13；主控设备 10 连接于云服务器 12 和门锁装置 11，智能终端 13 连接于云服务器 12；智能终端 13 用于在处于第一模式时，通过云服务器 12 发送解锁请求至主控设备 10；主控设备 10 用于在接收到解锁请求时，根据解锁请求判断是否允许解锁，并在判

定允许解锁时，控制门锁装置 11 解锁。其中，图 1 中仅示意出了一个智能终端 13，然并不以此为限。

[0033] 下面对本实施方式的门禁系统的实现细节进行具体的说明，以下内容仅为方便理解提供的实现细节，并非实施本方案的必须。

[0034] 本实施例中的主控设备 10 可以是一个小型工作站，或者可以是个人电脑等智能设备。门锁装置 11 可以包括一个微控制器、机械锁以及驱动机构；主控设备 10 控制门锁装置 11 解锁，具体可以为，主控设备 10 发送解锁命令至门锁装置 11 的微控制器，微控制器接收到解锁命令时通过驱动机构驱动机械锁打开以实现解锁。

[0035] 在一个例子中，如图 2 所示，云服务器 12 与主控设备 10 之间的通讯方式可以有多种，例如但不限于以下两种：广域网 WAN、窄带物联网 NB-IOT。智能终端 13 与主控设备之间的通讯方式，也可以由多种，除了基于云服务器 13 通讯，还可以基于近距离无线传输技术通讯；图 2 中示意出了两种近距离无线传输方式，蓝牙和无线局域网 WIFI；然并不以此为限，其他类型的近距离无线传输技术如红外线技术、微波技术等均可应用于本实施例中。

[0036] 智能终端 13 可以有多种不同模式，在不同模式中，选择不同的通讯路径发送解锁请求至主控设备，本实施例中智能终端 13 可以处于第一模式或第二模式。

[0037] 智能终端 13 在处于第一模式时，将解锁请求发送给云服务器 12，以通过云服务器 12 将解锁请求发送至主控设备 10。云服务器 12 接收到解锁请求时，可以选择 WAN 或 NB-IOT 的任意一条路径将解锁请求发送至门锁装置 11，这样可以在其中一条路径发生拥堵或者无法接通时，选择另一条路径发送解锁请

求；从而避免其中一条传输路径发生堵塞或中断时影响正常解锁。

[0038] 智能终端 13 在处于第二模式时，可以基于近距离无线传输技术发送解锁请求至主控设备 10；图 2 中所示的 WIFI 路径中设置一个独立的 WIFI 设备 14（如路由器）作为中转，用于拓宽 WIFI 的覆盖范围；然并不以此为限。

[0039] 本实施例中的门锁装置 11 可以应用于各种场景，如，门锁装置 11 可以安装在电影院、工厂仓库、地铁等公共场所的闸机位置；或者，也可以安装在保险箱等个人物品上。其中，当门锁装置 11 安装在保险箱等这类可移动设备上时，即使可移动设备被不法分子盗取，由于要基于主控设备进行解锁，而可移动设备被盗取后因为远离主控设备而无法与主控设备信号连接，因此不法分子无法通过对可移动设备采用软件侵入的方式非法解锁，在一定程度上提高了安全性（现有技术中，当采用近距离无线通讯技术向可移动设备发送解锁请求时，由门锁装置内的微控制器判断是否允许解锁，因此不法分子盗取可移动设备后，可以对门锁装置内的微控制器采用软件侵入的方式进行非法解锁）。

[0040] 本实施例中，主控设备 10 用于在接收到解锁请求时，根据解锁请求判断是否允许解锁，并在判定允许解锁时，控制门锁装置 11 解锁。在一个例子中，主控设备 10 可以根据解锁请求识别特征信息，特征信息可以包括发送解锁请求的用户的身份信息；主控设备 10 获取用户对应的门禁权限并至少根据获取的门禁权限判断是否允许解锁。具体的，主控设备 10 内可以储存有用户和门禁权限的对应关系，主控设备 10 根据该用户和门禁权限的对应关系获取发送解锁请求的用户对应的门禁权限。其中，用户的身份信息例如可以为用户的账号信息，以作为该用户身份的唯一标志；门禁权限可以为有解锁权限或无解锁权限，当用户对应的门禁权限为有解锁权限时，主控设备判定允许解锁并控制门锁装置

解锁；当用户对应的门禁权限为无解锁权限时，主控设备判定不允许解锁。

[0041] 在另一个例子中，特征信息可以包括解锁密码，主控设备 10 从解锁请求中识别出该解锁密码，并判断该解锁密码与预设的标准密码是否一致，若一致，则判定允许解锁。

[0042] 在又一个例子中，特征信息可以包含用户的身份信息和解锁密码，主控设备在判定用户对应的门禁权限为有解锁权限的情况下，再判断解锁密码与预设的标准密码是否一致；如果一致则允许解锁；否则不允许解锁。

[0043] 需要说明的是，本实施例对主控设备 10 根据解锁请求判断是否允许解锁的具体方式不作任何限制，以上仅为举例说明。

[0044] 本实施例中，由主控设备判断是否允许解锁，即主控设备 10 中储存了用于进行解锁判断的核心数据，核心数据如上面例子中用户和门禁权限的对应关系、标准密码以及具体的解锁判断方式等；而现有技术中由云服务器储存这些核心数据。由于本案中的主控设备相当于复杂网络结构中的边缘节点，相较于作为网络的中心节点的云服务器而言，边缘节点被非法入侵的难度较大，即核心数据在边缘节点中的安全性更高，因此本实施例可以提高门禁系统的安全性；并且，作为边缘节点的主控设备所要处理的业务相对较少，其处理速度也会相对较快。

[0045] 在一个例子中，门禁权限的权限类型可以包括但不限于以下类型的其中之一或任意组合：位置受限、时间受限、通行方向受限等。其中，位置受限是指只有在预设区域内才具有解锁权限；例如，可以将主控设备 10 设置成只允许基于近距离无线技术接收智能终端 13 的解锁请求，即智能终端 13 只有在近距离内（近距离无线技术的覆盖范围）才能发送解锁请求。时间受限是指只有在

预设时间段内才具有解锁权限；例如，可以将主控设备 10 内设置预设时间段，主控设备 10 记录解锁请求的接收时刻、或者解锁请求的特征信息中包含智能终端 13 记录的解锁请求的发送时刻，如果接收时刻或者发送时刻在预设时间段内，则允许解锁。通行方向受限是指只允许用户进入或离开，即对于可以双向通行的门禁系统，如有两个闸机通道，分别对应两个通行方向；该用户发送解锁请求后，主控设备只会解锁允许该用户通行的方向上的闸机。

[0046] 需要说明的是，本实施例的门禁系统除了支持在线解锁，也支持如 NFC、或指纹密码、或数字密码等离线解锁，即门锁装置上可以根据需要安装 NFC 模块、指纹识别模块、输入模块等，从而实现离线解锁。

[0047] 本申请第二实施例涉及一种门禁系统，第二实施例与第一实施例大致相同，区别之处在于，第二实施例中，请参考图 1 或图 2，云服务器 12 可以主动监控预设事件，以在预设事件发生时通知主控设备采取措施。

[0048] 具体的，云服务器 12 可以在监测到预设事件发生时，发送预警信号至主控设备 10，主控设备 10 还用于在接收到预警信号时，进入预设的控制模式。其中，云服务器 12 可以通过网络监测预设事件，预设事件可以是一些高危事件，例如洪水、地震、天体撞击、火灾等重大灾害；预设的控制模式可以但不限于如下方式：直接控制门锁装置解锁，或者无条件解锁；其中，无条件解锁是指只要接收到智能终端 13 发送的解锁请求，就控制门锁装置 11 解锁。或者，在预设的控制模式中，主控设备 10 还可以检测门锁装置 11 的内侧是否有人，如果有人的话，控制门锁装置 11 解锁，其中，主控设备 10 可以通过预先安装在门锁装置 11 的内侧的多个传感器来检测门锁装置 11 的内侧是否有人；门锁装置 11 的内侧可以理解为，例如门锁装置 11 安装在仓库的大门上，则门锁装置

11 的内侧是指仓库内部空间。

[0049] 例如，当发生洪水灾害时，相关部门可能会在某些网络平台上发表洪水灾害信息，或者，网络用户也可能在某些网络平台上及时告知其他网友；云服务器 12 可以被预设为对一些网络平台等信息渠道进行监控，当监控到关于预设事件的相关信息时，就会发出预警信号至主控设备 10。

[0050] 又例如，门锁装置 11 设置在一个仓库的大门上，仓库周围预设区域内安装有各类传感器以检测周边环境，各类传感器例如包括温度检测器、烟雾检测器等；当仓库周围预设区域内发生火灾时，各类传感器会发出异常信号；云服务器 12 监测到该些异常信号时，判定预设事件发生，并发出预警信号至主控设备 10。

[0051] 以上仅为举例，本实施例对预设事件的具体类型及其对应的预设的控制模式不作任何限制，可以根据需要设定。本实施例中，云服务器可以主动监测预设事件，并在预设事件发生时告知主控设备，从而使得主控设备进入预设的控制模式；可以满足更多的实际应用场景的需要。

[0052] 在一个例子中，云服务器 12 包含多个分布式站点；各分布式站点用于在监测到预设事件发生时，分别发送预警信号至主控设备 10。主控设备 10 用于在接收到各分布式站点发送的预警信号时，进入预设的控制模式。即，云服务器 12 为分布式结构，主控设备 10 需要同时接收到多个分布式站点的预警信号时才进入预设的控制模式，从而可以尽可能避免个别分布式站点监测错误而导致误判，可靠性更高。

[0053] 本申请第三实施例涉及一种门禁系统，第三实施例与第一实施例大致相同，区别之处在于，如图 3 所示，智能终端 13 可以包括管理员终端 13-1 和普

通用用户终端 13-2, 图 3 中对管理员终端 13-1 和普通用户终端 13-2 的数量仅是示例说明, 不作以此为限。如果在紧急事件发生时, 普通用户终端 13-2 不具备解锁权限, 那么普通用户终端 13-2 可以向管理员终端 13-1 发送紧急解锁请求; 管理员终端 13-1 用于对紧急解锁请求进行认证, 并将经过认证的紧急解锁请求发送至主控设备 10; 主控设备 10 在接收到经过认证的紧急解锁请求后, 控制门锁装置 11 解锁。其中, 图 3 中仅示意出了在遇到紧急事件, 普通用户终端 13-2 通过管理员终端 13-1 发送紧急解锁请求的传输路径, 但并不以此为限, 普通用户终端 13-2 也可以通过云服务器 12 或基于近距离无线传输技术发送解锁请求至主控设备 10。

[0054] 本实施例中, 普通用户终端 13-2 和管理员终端 13-1 对应的门禁权限不同。管理员终端 13-1 具备较高的门禁权限, 即, 主控设备 10 可以被设定为, 只要是接收到经过管理员终端 13-1 认证过的紧急解锁请求, 均会允许解锁。普通用户终端 13-2 不具有该门锁设备的解锁权限, 或者, 普通用户终端 13-2 的门禁权限包括位置受限或时间受限等限制类型, 导致在紧急事件发生时, 普通用户终端 13-2 不具备解锁权限。所以, 当普通用户终端 13-2 发现紧急事件发生时, 需要通过管理员终端 13-1 来向主控设备 10 请求解锁。

[0055] 例如, 门锁装置 11 设置在一个仓库的大门上, 仓库管理员使用的门禁账号对应于管理员终端 13-1, 仓库货物搬运人员使用的门禁账号对应于普通用户终端 13-2; 仓库货物搬运人员的门禁权限包括时间受限这一类型, 只有在上班时间段 (例如上午八点到下午四点这一时间段内) 才有解锁权限。当仓库货物搬运人员在非上班时间段发现紧急事件发生而此时仓库管理员不在现场时, 紧急事件例如为仓库内有人呼救, 仓库货物搬运人员可以通过普通用户终端 13-2

发送紧急解锁请求至仓库管理员的管理员终端 13-1，仓库管理员的管理员终端 13-1 对紧急解锁请求进行认证后，发送经过认证的紧急解锁请求发送至主控设备 10，主控设备 10 在接收到经过认证的紧急解锁请求后，控制门锁装置 11 解锁。其中，管理员终端 13-1 在接收到紧急解锁请求时，可以自动进行认证并发送经过认证的紧急解锁请求发送至主控设备 10；或者可以提醒仓库管理员进行手动认证并发送经过认证的紧急解锁请求发送至主控设备 10。

[0056] 需要说明的是，第三实施例也可以是在第二实施例基础上的改进。

[0057] 本申请第四实施例涉及一种门禁系统，第四实施例与第一实施例大致相同，区别之处在于，在第四实施例，如图 4 所示，门禁系统还包括连接于智能终端 13 的辅助定位设备 15；智能终端 13 还用于在处于第一模式时，通过辅助定位设备 15 获取智能终端 13 的定位信息，解锁请求包括定位信息。

[0058] 其中，辅助定位设备 15 例如但不限于卫星，智能终端 13 可以但不限于进行 GPS 定位以得到定位信息；凡是能够使得智能终端 13 获取定位信息的辅助定位设备 15 的类型均属于本实施例的保护范围。

[0059] 智能终端 13 在处于第一模式时，是通过云服务器 12 发送解锁请求至主控设备 10 的，即可以实现远程解锁；但对于有些用户，门禁权限被设置了位置受限；此时可以通过辅助定位设备 15 获取用户的定位信息，并将定位信息整合在解锁请求中一起发送至主控设备；从而主控设备 10 可以对这些基于云服务器 12 发送解锁请求的位置受限用户进行解锁允许判断。

[0060] 需要说明的是，第四实施例也可以是在第三实施例基础上的改进。

[0061] 本申请第五实施例涉及一种门禁系统，第五实施例与第四实施例大致相同，区别之处在于，在第五实施例，如图 5 所示，门禁系统还包括连接于主控

设备 10 的存储设备 16; 主控设备 10 还用于在根据解锁请求判断是否允许解锁后, 生成解锁请求的解锁记录, 并将解锁记录存储至存储设备 16; 其中, 解锁记录至少包括: 主控设备 10 根据解锁请求识别出的发送解锁请求的用户的身份信息, 以及是否解锁成功。

[0062] 本实施例中, 解锁记录中的是否解锁成功, 可以是: 主控设备 15 根据门禁权限判断出的结果, 即允许解锁或不允许解锁; 其中, 当主控设备 10 判断出允许解锁并控制门锁装置 11 解锁后, 门锁装置 11 还可以将表征解锁成功的反馈信息发送至主控设备 10, 当主控设备 10 接收到表征解锁成功的反馈信息时, 确定解锁成功。本实施例中的解锁记录还可以包括主控设备接收解锁请求的时间、控制门锁装置解锁的时间(如果允许解锁的话)等, 可以根据需要设定。

[0063] 在一个例子中, 门禁权限的权限类型还可以包含匿名权限; 主控设备 10 先识别用户的门禁权限是否包含匿名权限, 如果用户的门禁权限包含匿名权限, 那么不会生成解锁记录; 如果用户的门禁权限没有包含匿名权限, 那么生成解锁记录。即, 对于一些具有匿名权限的用户, 主控设备 10 不会对其解锁请求的过程进行记录。本实施例中进一步丰富了用户的门禁权限种类, 可以满足更多的实际应用场景的需求。

[0064] 本申请第六实施例涉及一种门禁系统的解锁方法, 应用于门禁系统中的主控设备, 门禁系统请参考图 1 或图 2, 门禁系统还包括云服务器、门锁装置以及至少一智能终端; 智能终端用于在处于第一模式时, 通过云服务器发送解锁请求至主控设备。

[0065] 如图 6 所示为本实施例中的门禁系统的解锁方法的流程图, 具体如下。

[0066] 步骤 101, 判断是否接收到解锁请求; 若是, 进入步骤 102; 若否, 重复

步骤 101。

[0067] 步骤 102, 根据解锁请求判断是否允许解锁; 若是, 进入步骤 103; 若否, 结束。

[0068] 步骤 103, 控制门锁装置解锁。

[0069] 如图 7 所示的一个例子中, 步骤 102, 具体包含如下子步骤:

[0070] 子步骤 1021, 根据解锁请求识别特征信息; 其中, 特征信息至少包括发送解锁请求的用户的身份信息。

[0071] 子步骤 1022, 获取用户对应的门禁权限。

[0072] 子步骤 1023, 至少根据获取的门禁权限判断是否允许解锁。

[0073] 本实施例中, 由主控设备判断是否允许解锁, 因此主控设备中储存了用于进行解锁判断的核心数据, 而现有技术中由云服务器储存这些核心数据(现有技术中由云服务器判断是否允许解锁); 由于本案中的主控设备相当于复杂网络结构中的边缘节点, 相较于作为网络的中心节点的云服务器而言, 边缘节点被非法入侵的难度较大, 即核心数据在边缘节点中的安全性更高, 因此本实施例可以提高门禁系统的安全性; 并且, 作为边缘节点的主控设备所要处理的业务相对较少, 其处理速度也会相对较快。

[0074] 不难发现, 本实施方式为与第一实施方式相对应的方法实施例, 本实施方式可与第一实施方式互相配合实施。第一实施方式中提到的相关技术细节在本实施方式中依然有效, 为了减少重复, 这里不再赘述。相应地, 本实施方式中提到的相关技术细节也可应用在第一实施方式中。

[0075] 本申请第七实施例涉及一种门禁系统的解锁方法, 第七实施例与第六实施例大致相同, 区别之处在于, 主控设备可以接收云服务器监测到预设事件发

生时发送的预警信号，并采取措施。

[0076] 如图 8 所示为本申请第七实施例的门禁系统的解锁方法的流程图，包括：

[0077] 步骤 201，判断是否接收到解锁请求；若是，进入步骤 202；若否，重复步骤 201。

[0078] 步骤 202，根据解锁请求判断是否允许解锁；若是，进入步骤 203；若否，进入 204。

[0079] 步骤 203，控制门锁装置解锁。

[0080] 步骤 204，判断是否接收到云服务器在监测到预设事件发生时发送的预警信号；若是，进入步骤 205；若否，重复步骤 204。

[0081] 步骤 205，进入预设的控制模式。

[0082] 其中，步骤 201~步骤 203 与第六实施例中的步骤 101~步骤 103 大致相同，此处不再赘述，不同之处在于还包含步骤 204~步骤 205。需要说明的是，步骤 201~步骤 203 用于实现门禁解锁，步骤 204~步骤 205 为实现预设事件发生时的门禁控制，两者执行顺序不限，即，实现门禁解锁和实现预设事件发生时的门禁控制可以并发执行，图 8 中只是示意性说明。

[0083] 本实施例中，云服务器可以主动监测预设事件，并在预设事件发生时告知主控设备，从而使得主控设备进入预设的控制模式；即主控设备可以在预设事件发生时采用预先设定好的门禁控制，可以满足更多的实际应用场景的需要。

[0084] 在一个例子中，云服务器包含多个分布式站点，各分布式站点用于在监测到预设事件发生时，分别发送预警信号至主控设备。主控设备在接收到各分布式站点发送的预警信号时，进入预设的控制模式；从而可以尽可能避免个别分布式站点监测错误而导致误判，可靠性更高。

[0085] 本实施方式为与第二实施方式相对应的方法实施例，本实施方式可与第二实施方式互相配合实施。第二实施方式中提到的相关技术细节在本实施方式中依然有效，为了减少重复，这里不再赘述。相应地，本实施方式中提到的相关技术细节也可应用在第二实施方式中。

[0086] 本申请第八实施例涉及一种门禁系统的解锁方法，第八实施例与第六实施例大致相同，区别之处在于，对于门禁权限被设置为位置受限的用户，可以结合用户的定位信息来判断是否允许解锁。

[0087] 本申请第八实施例的门禁系统的解锁方法与第六实施例中相比，步骤 102 包含的子步骤不同，如图 9 所示为本申请第八实施例中根据解锁请求判断是否允许解锁这一步骤的具体流程图。

[0088] 子步骤 3021，根据解锁请求识别特征信息；其中，特征信息至少包括发送解锁请求的用户的身份信息；

[0089] 子步骤 3022，获取用户对应的门禁权限；

[0090] 子步骤 3023，识别解锁请求的接收途径；若接收途径为通过云服务器接收，进入子步骤 3024；若基于近距离无线通讯技术接收，进入子步骤 3027；

[0091] 子步骤 3023 中，识别解锁请求的接收途径的具体方式，例如但不限于以下方式：主控设备具有多个接收模块，如与云服务器的通讯协议匹配的接收模块、与 WIFI 的通讯协议匹配的接收模块、与蓝牙通讯协议匹配的接收模块等，主控设备可以识别解锁请求从哪个接收模块接收，从而确定解锁请求的接收路径。如果是通过云服务器接收，那么要基于门禁权限是否包含位置受限来确定该用户是否可以远程解锁，即进入子步骤 3024。如果是基于 WIFI 或蓝牙这类近距离无线通讯技术接收，由于近距离无线通讯技术本身就要求用户在近距离

无线通讯所能覆盖的范围内才能接收到解锁请求，所以如果是基于近距离无线通讯技术接收的，用户必定在近距离无线通讯所能覆盖的范围内。

[0092] 子步骤 3024，判断门禁权限是否包含位置受限、特征信息是否包含用户的定位信息；若门禁权限包括位置受限，且特征信息包括用户的定位信息，进入子步骤 3025；若门禁权限包括位置受限，且特征信息未包括用户的定位信息，进入子步骤 3026；若门禁权限不包含位置受限，则进入子步骤 3027。

[0093] 子步骤 3025，根据用户的定位信息和预设的位置限制条件判断是否允许解锁；其中，用户的定位信息由智能终端通过辅助定位设备获取；

[0094] 子步骤 3026，不允许解锁。

[0095] 子步骤 3027，根据门禁权限判断是否允许解锁。

[0096] 其中，步骤 3021~步骤 3022 与第六实施例中的步骤 1021~步骤 1022 大致相同，此处不再赘述，不同之处在于子步骤 3023~子步骤 3027。

[0097] 即，当门禁权限中包含位置受限时，表示该用户不能进行远程解锁；如果解锁请求中没有包含用户的定位信息，那么不允许解锁；如果解锁请求中包含用户的定位信息，那么判断该定位信息是否满足位置限制条件，该位置限制条件例如为一个预设的区域，用户位于该预设的区域内，则判定允许解锁。

[0098] 本实施方式为与第四实施方式相对应的方法实施例，本实施方式可与第四实施方式互相配合实施。第四实施方式中提到的相关技术细节在本实施方式中依然有效，为了减少重复，这里不再赘述。相应地，本实施方式中提到的相关技术细节也可应用在第四实施方式中。

[0099] 需要说明的是，本实施例也可以是在第七实施例基础上的改进。

[00100] 本申请第九实施例涉及一种门禁系统的解锁方法，第九实施例与第六

实施例大致相同，区别之处在于，主控设备 10 还可以生成解锁请求的解锁记录，并将解锁记录存储至存储设备 16。

[00101] 如图 10 是根据本申请第九实施例的门禁系统的解锁方法的一个例子流程图，具体如下。

[00102] 步骤 401，判断是否接收到解锁请求；若是，进入步骤 402；若否，重复步骤 401。

[00103] 步骤 402，根据解锁请求判断是否允许解锁；若是，进入步骤 403；若否，结束。

[00104] 步骤 403，控制门锁装置解锁。

[00105] 步骤 404，判断主控设备根据解锁请求获取的用户对应的门禁权限中是否包含匿名权限；若否，进入步骤 405；若是，结束。

[00106] 步骤 405，生成解锁请求的解锁记录，并将解锁记录存储至存储设备；其中，解锁记录至少包括：主控设备根据解锁请求识别出的发送解锁请求的用户身份信息，以及是否解锁成功。

[00107] 其中，步骤 401~步骤 403 与第六实施例中的步骤 101~步骤 103 大致相同，此处不作赘述；不同之处在于还包括步骤 404、步骤 405。

[00108] 本实施例中，门禁权限的类型中包含匿名权限这一选项，因此要判断用户的门禁权限中是否包含匿名权限，才确定是否要生成该用户的解锁记录；在其他例子中，如果门禁权限的类型中没有包含匿名权限这一选项，那么无需执行步骤 404，即对接收到的每条解锁请求都生成对应的解锁记录。另外，本实施例中对步骤 403、步骤 404、步骤 405 的执行顺序不限，可以根据需要或实际情况执行。

[00109] 需要说明的是,第九实施例也可以是在第七或第八实施例基础上的改进。

[00110] 本实施方式为与第五实施方式相对应的方法实施例,本实施方式可与第五实施方式互相配合实施。第五实施方式中提到的相关技术细节在本实施方式中依然有效,为了减少重复,这里不再赘述。相应地,本实施方式中提到的相关技术细节也可应用在第五实施方式中。

[00111] 本申请第十实施例涉及一种处理芯片,如图 11 所示,处理芯片 110 与至少一存储器 111 连接,存储器 111 存储有可被处理芯片 110 执行的指令,指令被处理芯片 110 执行,以使处理芯片 110 能够执行上述方法实施例。

[00112] 本申请第十一实施例涉及一种主控设备,包括上述处理芯片。

[00113] 本领域的普通技术人员可以理解,上述各实施例是实现本申请的具体实施例,而在实际应用中,可以在形式上和细节上对其作各种改变,而不偏离本申请的精神和范围。

权利要求书

1、一种门禁系统，其特征在于，包括：主控设备、门锁装置、云服务器以及至少一智能终端；所述主控设备连接于所述云服务器和所述门锁装置，所述智能终端连接于所述云服务器；

所述智能终端用于在处于第一模式时，通过所述云服务器发送解锁请求至所述主控设备；

所述主控设备用于在接收到所述解锁请求时，根据所述解锁请求判断是否允许解锁，并在判定允许解锁时，控制所述门锁装置解锁。

2、如权利要求1所述的门禁系统，其特征在于，所述云服务器还用于在监测到预设事件发生时，发送预警信号至所述主控设备；所述主控设备还用于在接收到所述预警信号时，进入预设的控制模式。

3、如权利要求2所述的门禁系统，其特征在于，所述云服务器包含多个分布式站点；

各所述分布式站点用于在监测到所述预设事件发生时，分别发送所述预警信号至所述主控设备；

所述主控设备用于在接收到各所述分布式站点发送的所述预警信号时，进入预设的控制模式。

4、如权利要求1所述的门禁系统，其特征在于，所述智能终端包括管理员终端和普通用户终端；

所述普通用户终端用于在预设的紧急事件发生时，向所述管理员终端发送紧急解锁请求；其中，在所述紧急事件发生时，所述普通用户终端不具备解锁权限；

所述管理员终端用于对所述紧急解锁请求进行认证，并将经过认证的所述紧急解锁请求发送至所述主控设备；

所述主控设备在接收到经过认证的所述紧急解锁请求后，控制所述门锁装置解锁。

5、如权利要求1所述的门禁系统，其特征在于，所述门禁系统还包括连接于所述智能终端的辅助定位设备；

所述智能终端还用于在处于所述第一模式时，通过所述辅助定位设备获取所述智能终端的定位信息，所述解锁请求包括所述定位信息。

6、如权利要求1所述的门禁系统，其特征在于，所述门禁系统还包括连接于所述主控设备的存储设备；

所述主控设备还用于在根据所述解锁请求判断是否允许解锁后，生成所述解锁请求的解锁记录，并将所述解锁记录存储至所述存储设备；

其中，所述解锁记录至少包括：所述主控设备根据所述解锁请求识别出的发送所述解锁请求的用户的信息，以及是否解锁成功。

7、如权利要求1所述的门禁系统，其特征在于，所述门锁装置安装于可移动设备中。

8、如权利要求1所述的门禁系统，其特征在于，所述智能终端还用于在处于第二模式时，基于近距离无线传输技术发送所述解锁请求至所述主控设备。

9、一种门禁系统的解锁方法，其特征在于，应用于所述门禁系统中的主控设备，所述门禁系统还包括云服务器、门锁装置以及至少一智能终端；所述智能终端用于在处于第一模式时，通过所述云服务器发送解锁请求至所述主控设备；所述解锁方法包括：

当接收到所述解锁请求时，根据所述解锁请求判断是否允许解锁；

当判定允许解锁时，控制所述门锁装置解锁。

10、如权利要求 9 所述的门禁系统的解锁方法，其特征在于，还包括：

当接收到所述云服务器在监测到预设事件发生时发送的预警信号时，进入预设的控制模式。

11、如权利要求 10 所述的门禁系统的解锁方法，其特征在于，所述云服务器包括多个分布式站点；

所述接收到所述云服务器在监测到预设事件发生时发送的预警信号，具体为，接收到各所述分布式站点在监测到预设事件发生时分别发送的所述预警信号。

12、如权利要求 9 所述的门禁系统的解锁方法，其特征在于，所述根据所述解锁请求判断是否允许解锁，包括：

根据所述解锁请求识别特征信息；其中，所述特征信息至少包括发送所述解锁请求的用户的身份信息；

获取所述用户对应的门禁权限；

至少根据获取的所述门禁权限判断是否允许解锁。

13、如权利要求 12 所述的门禁系统的解锁方法，其特征在于，所述智能终端还用于在处于第二模式时，基于近距离无线传输技术发送所述解锁请求至所述主控设备；

在所述至少根据获取的所述门禁权限判断是否允许解锁之前，还包括：识别所述解锁请求的接收途径；

若所述接收途径为通过所述云服务器接收，则所述至少根据获取的所述门禁权限判断是否允许解锁，包括：

若所述门禁权限包括位置受限，且所述特征信息包括所述用户的定位信息，则根据所述用户的定位信息和预设的位置限制条件判断是否允许解锁；其中，所述用户的定位信息由所述智能终端通过辅助定位设备获取；

若所述门禁权限包括位置受限，且所述特征信息未包括所述用户的定位信息，判定为不允许解锁。

14、如权利要求 9 所述的门禁系统的解锁方法，其特征在于，所述门禁系统还包括存储设备；

在所述根据所述解锁请求判断是否允许解锁之后，还包括：

生成所述解锁请求的解锁记录，并将所述解锁记录存储至所述存储设备；其中，所述解锁记录至少包括：所述主控设备根据所述解锁请求识别出的发送所述解锁请求的用户的身份信息，以及是否解锁成功。

15、如权利要求 14 所述的门禁系统的解锁方法，其特征在于，在所述生成所述解锁请求的解锁记录，并将所述解锁记录存储至所述存储设备之前，还包括：

判定所述主控设备根据所述解锁请求获取的所述用户对应的门禁权限中不包含匿名权限。

16、如权利要求 12 所述的门禁系统的解锁方法，其特征在于，所述门禁权限的权限类型包括以下类型的其中之一或任意组合：位置受限、时间受限、匿名权限、通行方向受限。

17、一种处理芯片，其特征在于，与至少一存储器连接，所述存储器存储有可被所述处理芯片执行的指令，所述指令被所述处理芯片执行，以使所述处理芯片能够执行如权利要求 9 至 16 中任一项所述的门禁系统的解锁方法。

18、一种主控设备，其特征在于，包括权利要求 17 所述的处理芯片。

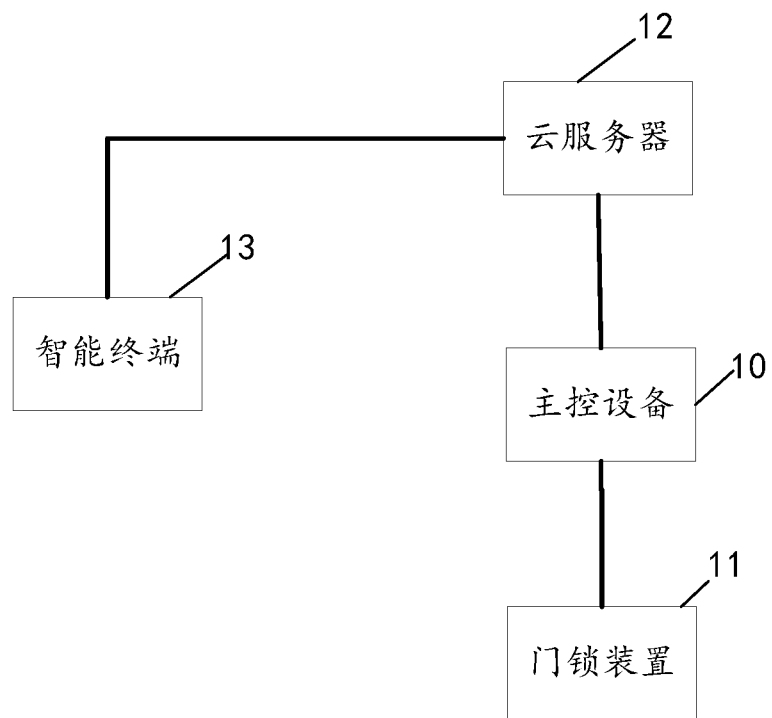


图 1

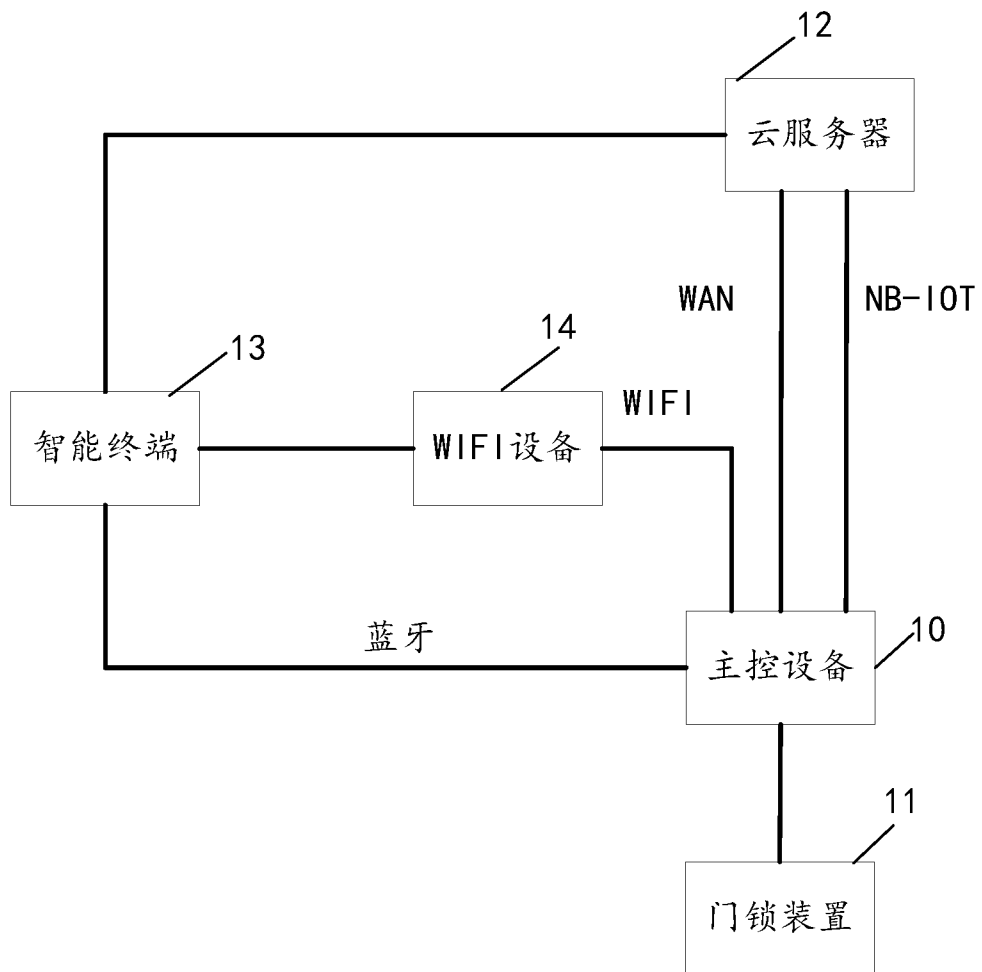


图 2

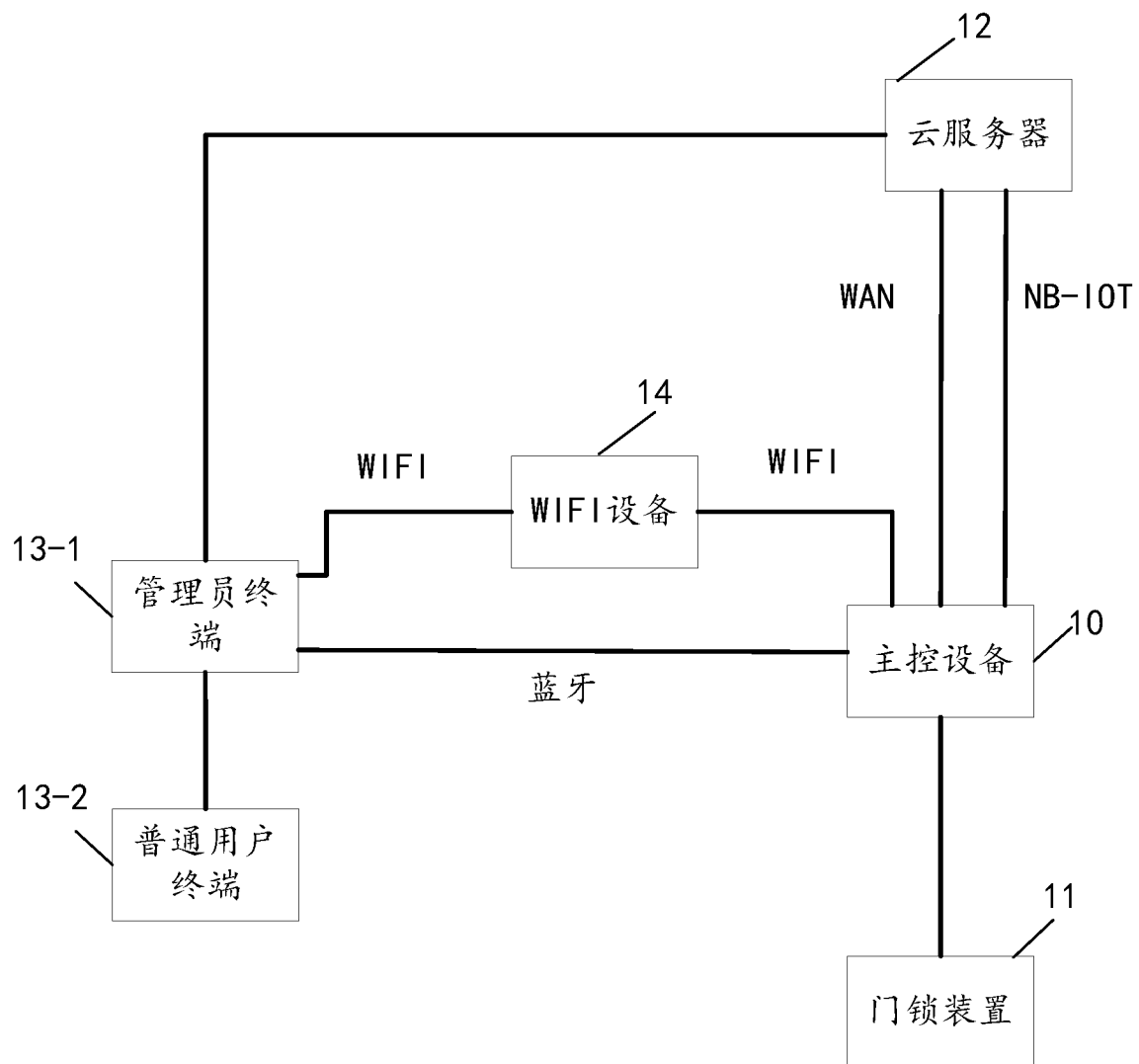


图 3

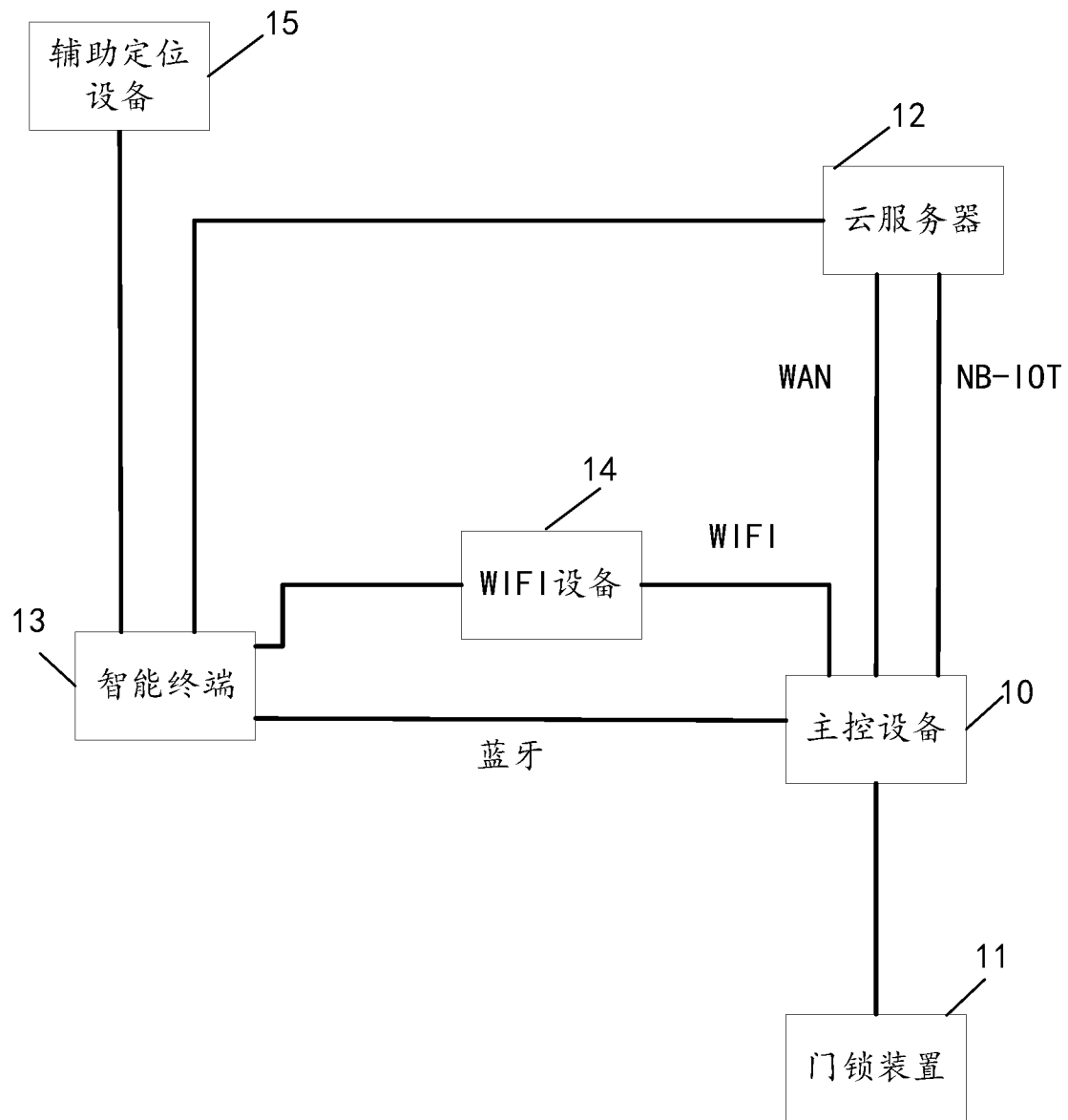


图 4

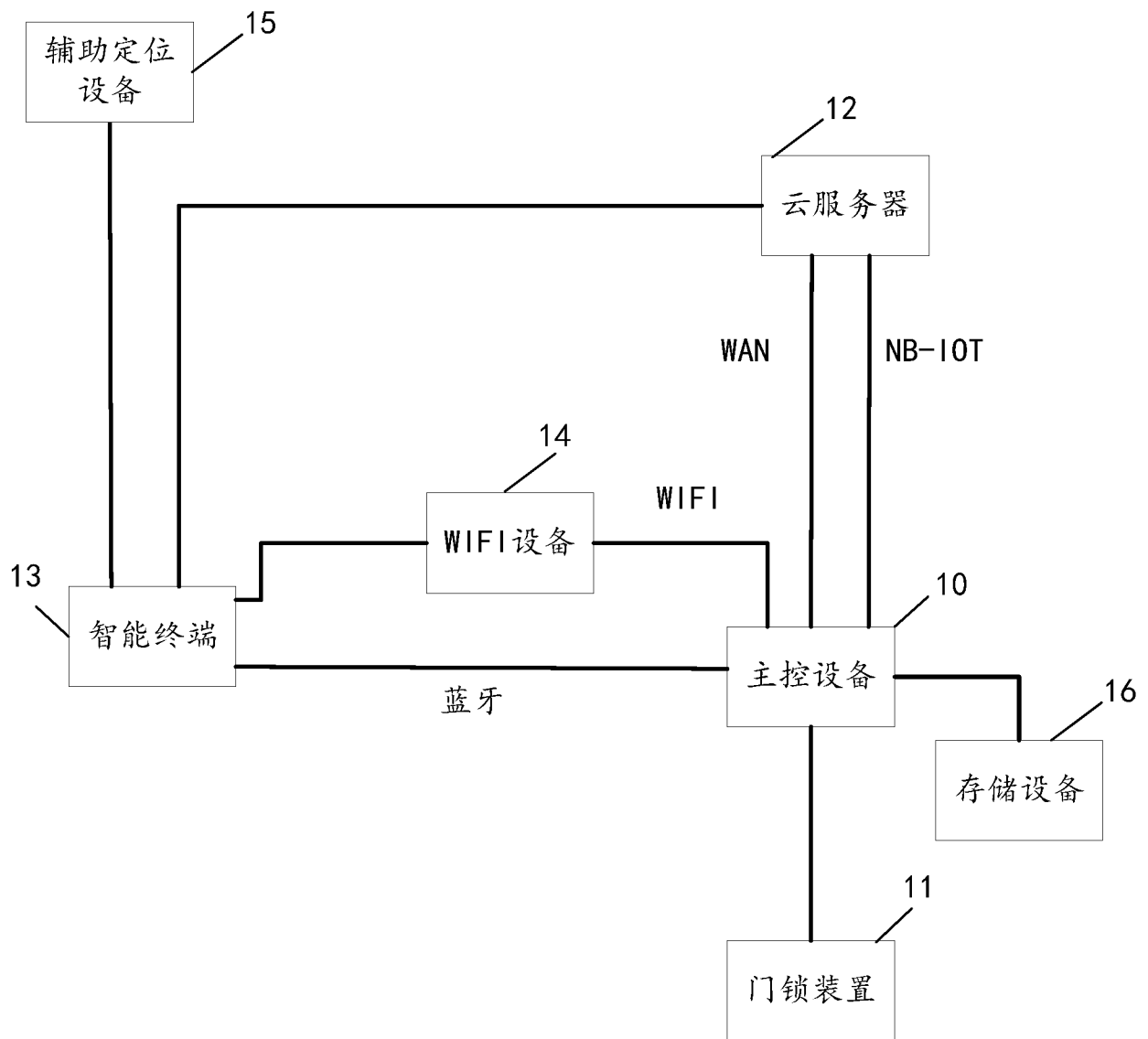


图 5

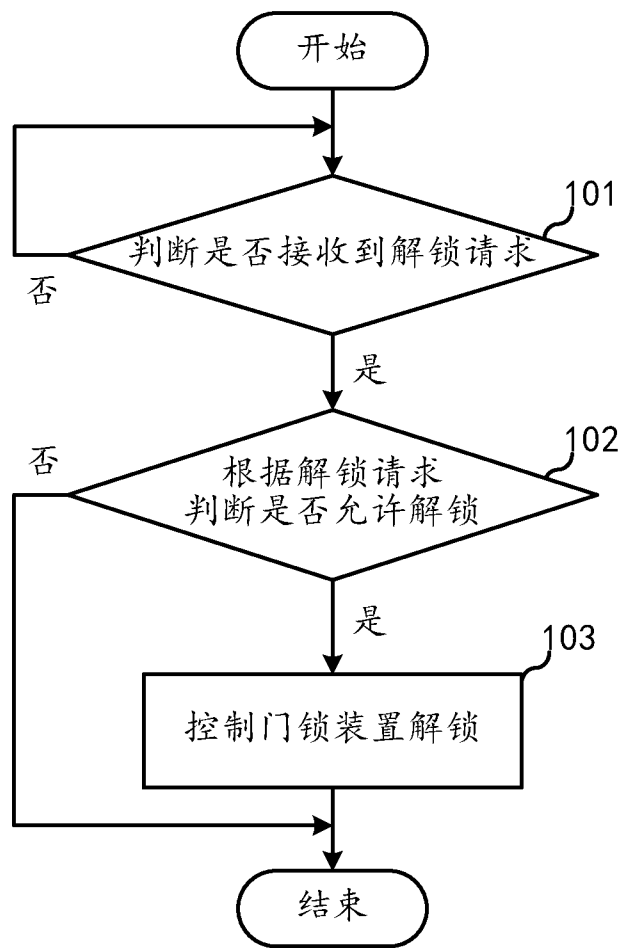


图 6

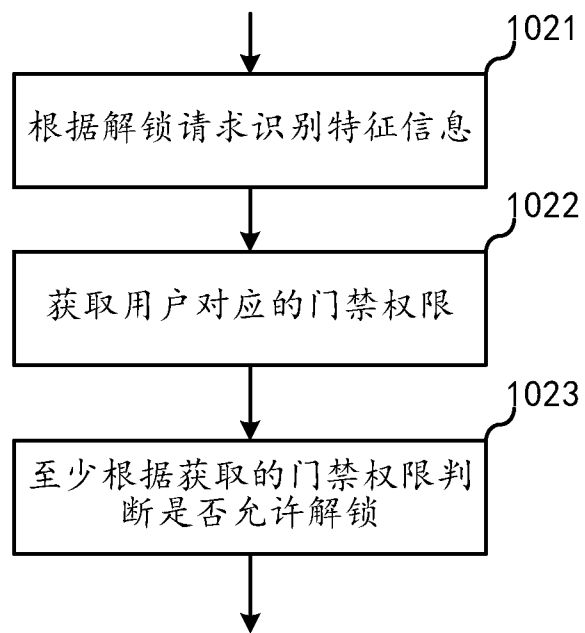


图 7

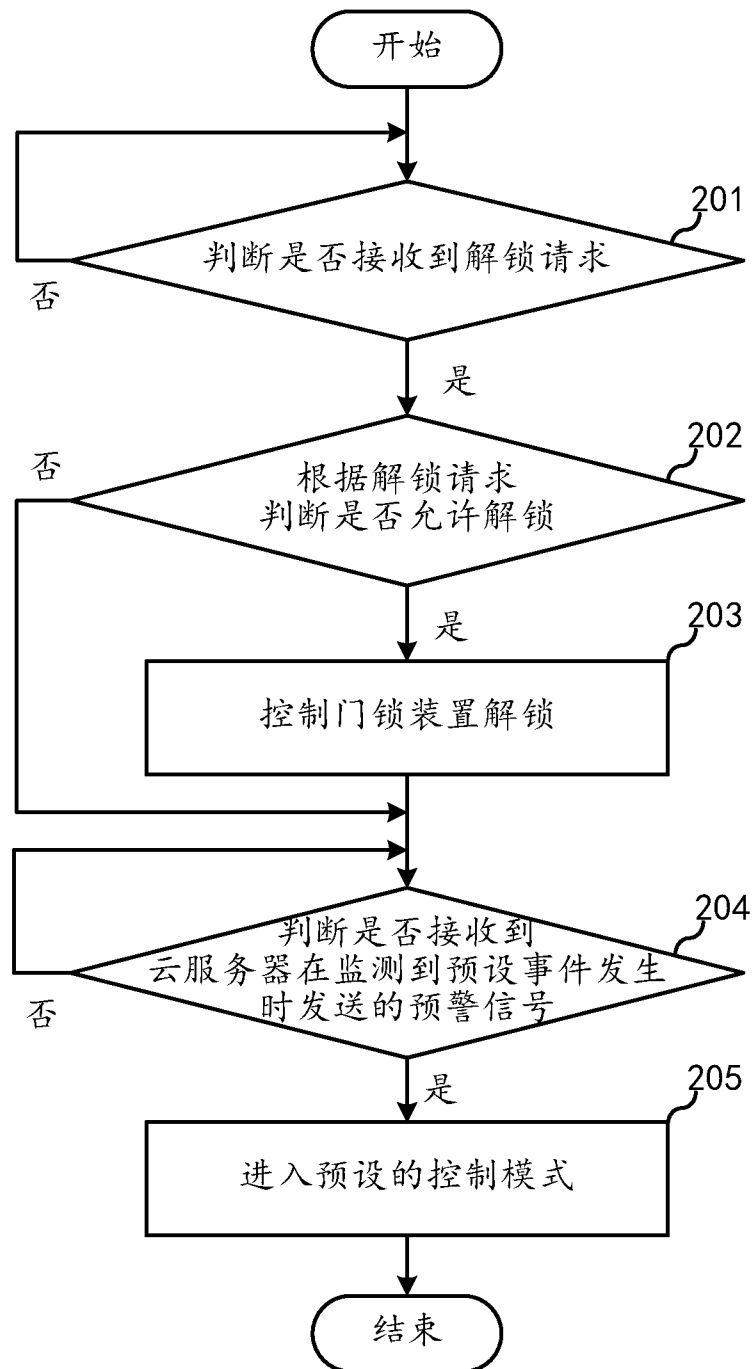


图 8

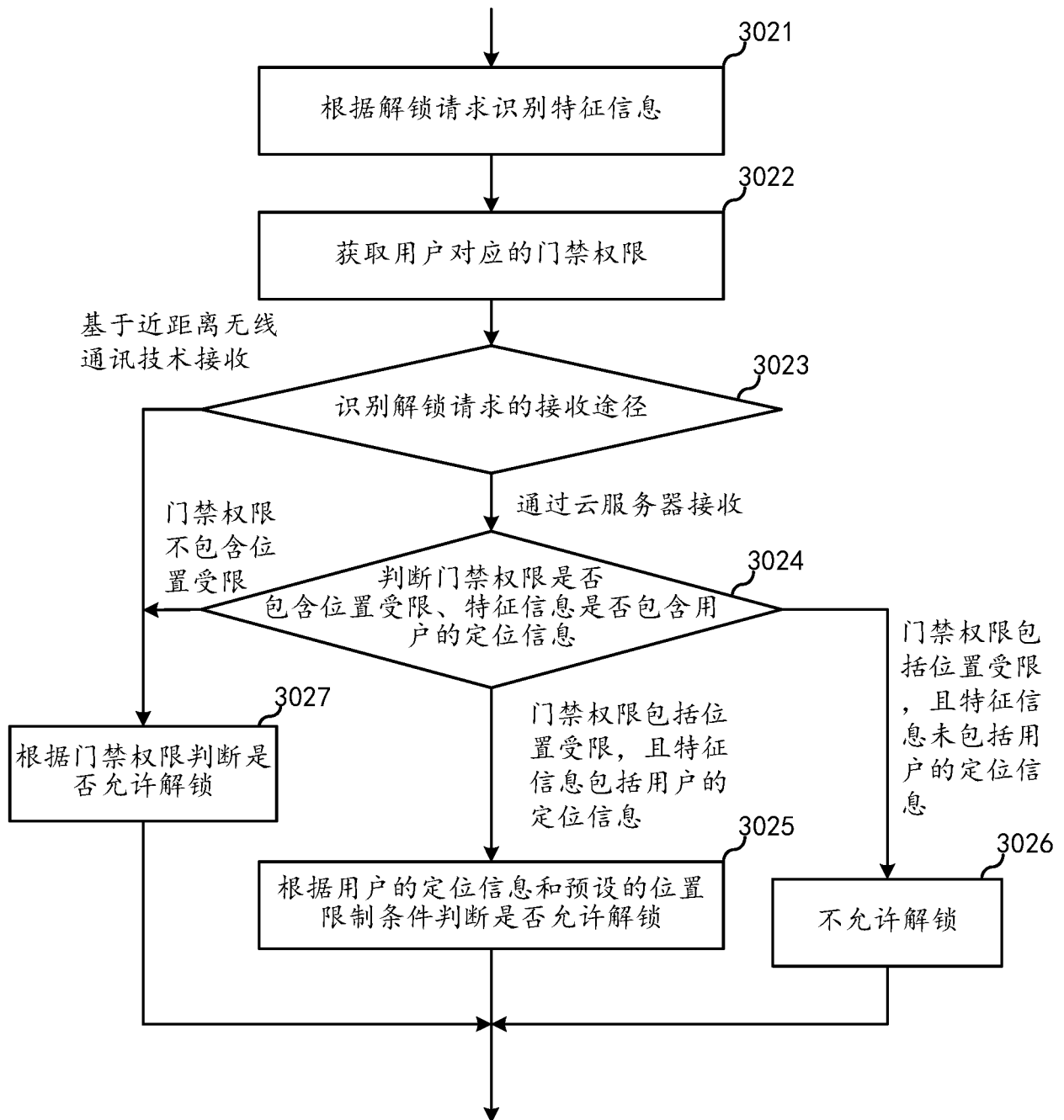


图 9

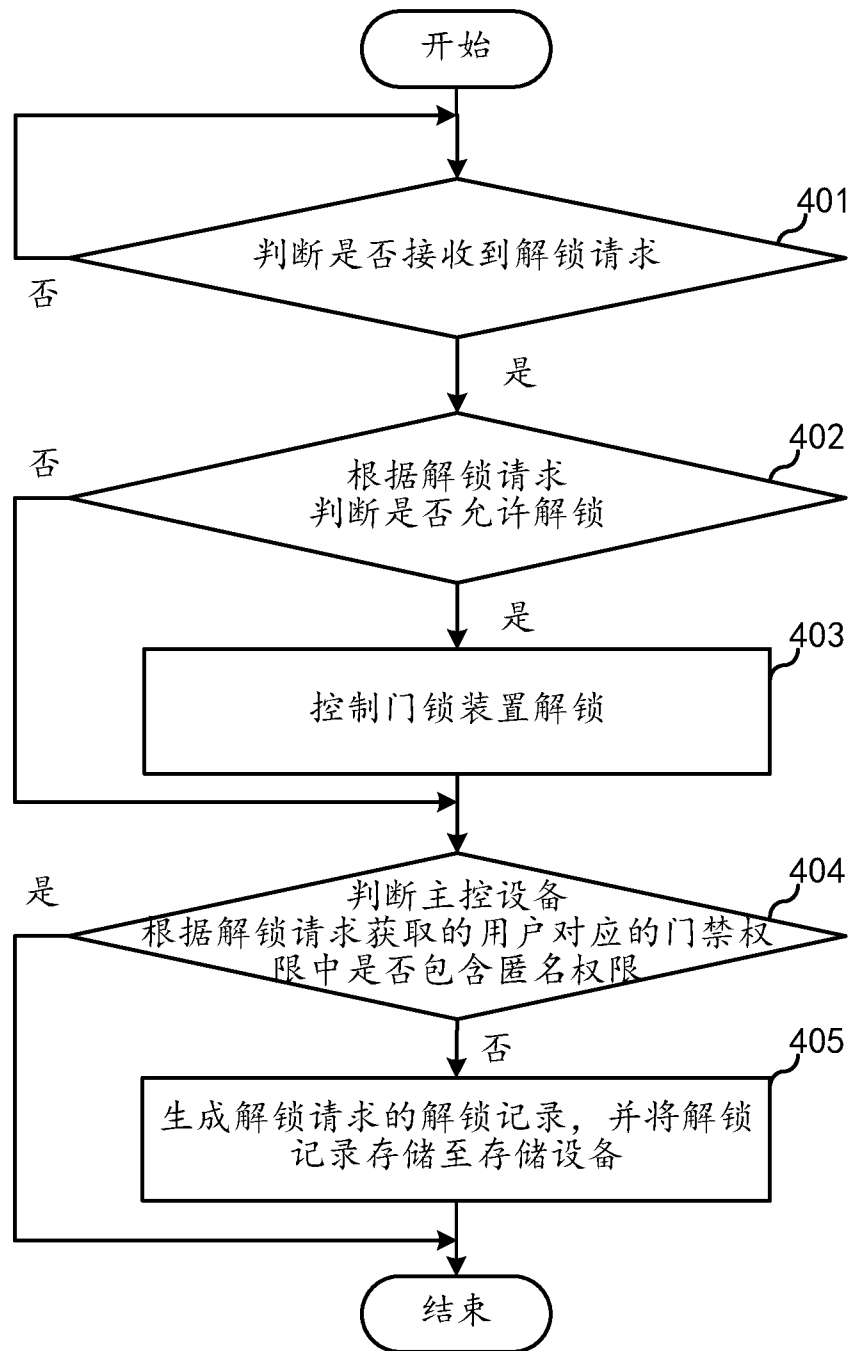


图 10

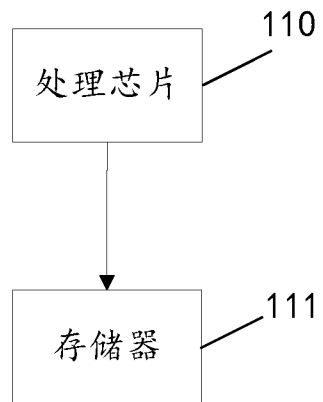


图 11

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2019/075210

A. CLASSIFICATION OF SUBJECT MATTER

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

G07C 9; H04L 29

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)

CNABS; CNTXT; VEN: 锁, 门禁, 解锁, 云, 服务器, 主控, 主机, 工作站, 位置, 定位, GPS, lock+, unlock+, access, cloud, server, control+, station, location, position, GPS

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 108547514 A (GREE ELECTRIC APPLIANCES, INC. OF ZHUHAI) 18 September 2018 (2018-09-18) description, paragraphs 0058-0126, and figures 1-6	1, 4, 6-9, 12, 14-15, 17-18
Y	CN 108547514 A (GREE ELECTRIC APPLIANCES, INC. OF ZHUHAI) 18 September 2018 (2018-09-18) description, paragraphs 0058-0126, and figures 1-6	2-3, 5, 10-11, 13, 16
Y	CN 107492173 A (QINGDAO YIFANGDE INTERNET OF THINGS TECHNOLOGY CO., LTD.) 19 December 2017 (2017-12-19) description, paragraphs 0017-0036, and figures 1-2	2-3, 10-11
Y	CN 106447850 A (GREAT WALL MOTOR COMPANY LIMITED) 22 February 2017 (2017-02-22) description, paragraphs 0056-0057	5, 13, 16
X	CN 106327648 A (BEIJING UPVALUE INTELLECTUAL PROPERTY CONSULTANT CO., LTD.) 11 January 2017 (2017-01-11) description, paragraphs 0046-0087, and figures 1-3	1, 6-9, 12, 14-15, 17-18
A	US 2018108192 A1 (GATE LABS INC.) 19 April 2018 (2018-04-19) entire document	1-18



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

12 November 2019

Date of mailing of the international search report

21 November 2019

Name and mailing address of the ISA/CN

China National Intellectual Property Administration
No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing
100088
China

Facsimile No. (86-10)62019451

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2019/075210

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN	108547514	A	18 September 2018	None	
CN	107492173	A	19 December 2017	None	
CN	106447850	A	22 February 2017	None	
CN	106327648	A	11 January 2017	None	
US	2018108192	A1	19 April 2018	None	

国际检索报告

国际申请号

PCT/CN2019/075210

A. 主题的分类 G07C 9/00(2006.01)i; H04L 29/08(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) G07C 9; H04L 29 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)) CNABS;CNTXT;VEN:锁, 门禁, 解锁, 云, 服务器, 主控, 主机, 工作站, 位置, 定位, GPS, lock+, unlock+, access, cloud, server, control+, station, location, position, GPS																							
C. 相关文件 <table border="1"> <thead> <tr> <th>类 型*</th> <th>引用文件, 必要时, 指明相关段落</th> <th>相关的权利要求</th> </tr> </thead> <tbody> <tr> <td>X</td> <td>CN 108547514 A (珠海格力电器股份有限公司) 2018年 9月 18日 (2018 - 09 - 18) 说明书第0058-0126段、附图1-6</td> <td>1, 4, 6-9, 12, 14-15, 17-18</td> </tr> <tr> <td>Y</td> <td>CN 108547514 A (珠海格力电器股份有限公司) 2018年 9月 18日 (2018 - 09 - 18) 说明书第0058-0126段、附图1-6</td> <td>2-3, 5, 10-11, 13, 16</td> </tr> <tr> <td>Y</td> <td>CN 107492173 A (青岛易方德物联科技有限公司) 2017年 12月 19日 (2017 - 12 - 19) 说明书第0017-0036段、附图1-2</td> <td>2-3, 10-11</td> </tr> <tr> <td>Y</td> <td>CN 106447850 A (长城汽车股份有限公司) 2017年 2月 22日 (2017 - 02 - 22) 说明书第0056-0057段</td> <td>5, 13, 16</td> </tr> <tr> <td>X</td> <td>CN 106327648 A (北京厚文知识产权顾问有限公司) 2017年 1月 11日 (2017 - 01 - 11) 说明书第0046-0087段、附图1-3</td> <td>1, 6-9, 12, 14-15, 17-18</td> </tr> <tr> <td>A</td> <td>US 2018108192 A1 (GATE LABS INC) 2018年 4月 19日 (2018 - 04 - 19) 全文</td> <td>1-18</td> </tr> </tbody> </table>			类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求	X	CN 108547514 A (珠海格力电器股份有限公司) 2018年 9月 18日 (2018 - 09 - 18) 说明书第0058-0126段、附图1-6	1, 4, 6-9, 12, 14-15, 17-18	Y	CN 108547514 A (珠海格力电器股份有限公司) 2018年 9月 18日 (2018 - 09 - 18) 说明书第0058-0126段、附图1-6	2-3, 5, 10-11, 13, 16	Y	CN 107492173 A (青岛易方德物联科技有限公司) 2017年 12月 19日 (2017 - 12 - 19) 说明书第0017-0036段、附图1-2	2-3, 10-11	Y	CN 106447850 A (长城汽车股份有限公司) 2017年 2月 22日 (2017 - 02 - 22) 说明书第0056-0057段	5, 13, 16	X	CN 106327648 A (北京厚文知识产权顾问有限公司) 2017年 1月 11日 (2017 - 01 - 11) 说明书第0046-0087段、附图1-3	1, 6-9, 12, 14-15, 17-18	A	US 2018108192 A1 (GATE LABS INC) 2018年 4月 19日 (2018 - 04 - 19) 全文	1-18
类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求																					
X	CN 108547514 A (珠海格力电器股份有限公司) 2018年 9月 18日 (2018 - 09 - 18) 说明书第0058-0126段、附图1-6	1, 4, 6-9, 12, 14-15, 17-18																					
Y	CN 108547514 A (珠海格力电器股份有限公司) 2018年 9月 18日 (2018 - 09 - 18) 说明书第0058-0126段、附图1-6	2-3, 5, 10-11, 13, 16																					
Y	CN 107492173 A (青岛易方德物联科技有限公司) 2017年 12月 19日 (2017 - 12 - 19) 说明书第0017-0036段、附图1-2	2-3, 10-11																					
Y	CN 106447850 A (长城汽车股份有限公司) 2017年 2月 22日 (2017 - 02 - 22) 说明书第0056-0057段	5, 13, 16																					
X	CN 106327648 A (北京厚文知识产权顾问有限公司) 2017年 1月 11日 (2017 - 01 - 11) 说明书第0046-0087段、附图1-3	1, 6-9, 12, 14-15, 17-18																					
A	US 2018108192 A1 (GATE LABS INC) 2018年 4月 19日 (2018 - 04 - 19) 全文	1-18																					
☐ 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 2019年 11月 12日		国际检索报告邮寄日期 2019年 11月 21日																					
ISA/CN的名称和邮寄地址 中国国家知识产权局(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		授权官员 孙培安 电话号码 86-(010)-62085800																					

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2019/075210

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	108547514	A	2018年 9月 18日	无	
CN	107492173	A	2017年 12月 19日	无	
CN	106447850	A	2017年 2月 22日	无	
CN	106327648	A	2017年 1月 11日	无	
US	2018108192	A1	2018年 4月 19日	无	