

(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
2024 年 2 月 1 日 (01.02.2024)



(10) 国际公布号
WO 2024/021908 A1

(51) 国际专利分类号:

H04L 43/0817 (2022.01) **G07C 9/00** (2020.01)

(21) 国际申请号:

PCT/CN2023/099363

(22) 国际申请日:

2023 年 6 月 9 日 (09.06.2023)

(25) 申请语言:

中文

(26) 公布语言:

中文

(30) 优先权:

202210894160.X 2022年7月27日 (27.07.2022) CN

(71) 申请人: 深圳 **TCL** 新技术有限公司
(**SHENZHEN TCL NEW TECHNOLOGY CO., LTD.**)
[CN/CN]; 中国广东省深圳市南山区西丽街道中山园路 1001 号国际 E 城 D4 栋 9 楼,
Guangdong 518052 (CN)。

(72) 发明人: 罗康(**LUO, Kang**); 中国广东省深圳市南山区西丽街道中山园路 1001 号国际 E 城 D4 栋 9 楼,
Guangdong 518052 (CN)。黎明德(**LI, Mingde**); 中

国广东省深圳市南山区西丽街道中山园路 1001 号
国际 E 城 D4 栋 9 楼, Guangdong 518052 (CN)。

(74) 代理人: 深圳紫藤知识产权代理有限公司 (**PURPLEVINE INTELLECTUAL PROPERTY (SHENZHEN) CO., LTD.**); 中国广东省深圳市南山区粤海街道大冲社区华润置地大厦 C 座 2901, Guangdong 518052 (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, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, MG, MK, MN, MU, 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, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, 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, CV, GH, GM, KE, LR, LS, MW, MZ,

(54) **Title:** DOOR LOCK SECURITY ASSESSMENT METHOD AND RELATED DEVICE

(54) 发明名称: 门锁安全评估方法以及相关设备

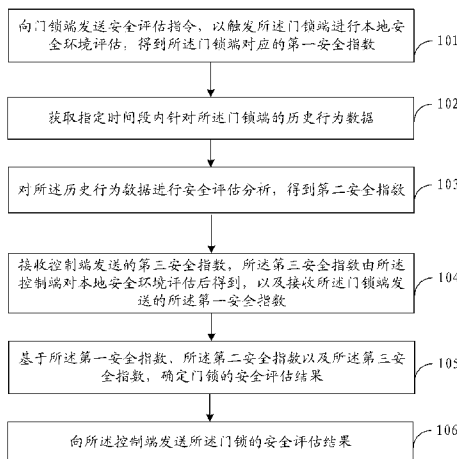


图 1b

(57) **Abstract:** A door lock security assessment method and a related device. The method may comprise: sending a security assessment instruction to a door lock end (12), so as to trigger the door lock end (12) to perform local security environment assessment to obtain a first security index corresponding to the door lock end (12); acquiring historical behavior data for the door lock end (12) within a specified time period; performing security assessment analysis on the historical behavior data to obtain a second security index; receiving a third security index, which is sent by a control end (10), wherein the third security index is obtained by the control end (10) after performing local security environment assessment, and receiving the first security index, which is sent by the door lock end (12); determining a security assessment result of a door lock on the basis of the first security index, the second security index and the third security index; and sending the security assessment result of the door lock to the control end (10). The security of a door lock is assessed in view of three aspects, i.e., a door lock end (12), a control end (10) and historical behavior data, such that the accuracy of a security assessment result corresponding to the door lock is improved.

- 101 Send a security assessment instruction to a door lock end, so as to trigger the door lock end to perform local security environment assessment to obtain a first security index corresponding to the door lock end
- 102 Acquire historical behavior data for the door lock end within a specified time period
- 103 Perform security assessment analysis on the historical behavior data to obtain a second security index
- 104 Receive a third security index, which is sent by a control end, wherein the third security index is obtained by the control end after performing local security environment assessment, and receive the first security index, which is sent by the door lock end
- 105 Determine a security assessment result of a door lock on the basis of the first security index, the second security index and the third security index
- 106 Send the security assessment result of the door lock to the control end

NA, RW, SC, 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, ME, 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))。

(57) 摘要：一种门锁安全评估方法以及相关设备，可以向门锁端（12）发送安全评估指令，以触发门锁端（12）进行本地安全环境评估，得到门锁端（12）对应的第一安全指数；获取指定时间段内针对门锁端（12）的历史行为数据；对历史行为数据进行安全评估分析，得到第二安全指数；接收控制端（10）发送的第三安全指数，第三安全指数由控制端（10）对本地安全环境评估后得到，以及接收门锁端（12）发送的第一安全指数；基于第一安全指数、第二安全指数以及第三安全指数，确定门锁的安全评估结果；向控制端（10）发送门锁的安全评估结果。结合门锁端（12）、控制端（10）以及历史行为数据三个方面，对门锁的安全性进行评估，提高了门锁对应的安全评估结果的准确性。

门锁安全评估方法以及相关设备

本申请要求于 2022 年 7 月 27 日提交中国专利局、申请号为 202210894160.X、发明名称为“门锁安全评估方法以及相关设备”的中国专利申请

申请的优先权，其全部内容通过引用结合在本申请中。

5 技术领域

本申请涉及智能电子设备技术领域，具体涉及一种门锁安全评估方法以及相关设备。

背景技术

随着智能门锁越来越普及，其安全性受到越来越多的挑战，消费者越来越关心智能门锁的安全性。

在目前的相关技术中，一般只对门锁端进行安全评估分析，得到安全评估结果，用户再根据安全评估结果对门锁进行安全设置；这样的评估方法较为简单，得到的安全评估结果的准确性相对较低。

发明内容

15 本申请实施例提供一种门锁安全评估方法以及相关设备，相关设备可以包括门锁安全评估装置、电子设备、计算机可读存储介质和计算机程序产品，可以提高门锁对应的安全评估结果的准确性。

本申请实施例提供一种门锁安全评估方法，包括：

20 向门锁端发送安全评估指令，以触发所述门锁端进行本地安全环境评估，得到所述门锁端对应的第一安全指数；

获取指定时间段内针对所述门锁端的历史行为数据；

对所述历史行为数据进行安全评估分析，得到第二安全指数；

接收控制端发送的第三安全指数，所述第三安全指数由所述控制端对本地安全环境评估后得到，以及接收所述门锁端发送的所述第一安全指数；

25 基于所述第一安全指数、所述第二安全指数以及所述第三安全指数，确定门锁的安全评估结果；及

向所述控制端发送所述门锁的安全评估结果。

本申请实施例提供另一种门锁安全评估方法，包括：

在接收到安全评估指令时，对本地环境进行安全评估，得到第三安全指数；

将所述第三安全指数发送给服务器，以触发所述服务器获取第一安全指数
5 和第二安全指数，其中，所述第一安全指数由门锁端对相应的本地环境进行安全评估后得到，所述第二安全指数由所述服务器对指定时间段内所述门锁端的历史行为数据进行安全评估后得到；及

接收所述服务器发送的安全评估结果，其中，所述安全评估结果由所述服务器基于所述第一安全指数、所述第二安全指数以及所述第三安全指数计算得到。

10 本申请实施例提供另一种门锁安全评估方法，包括：

接收服务器发送的安全评估指令，其中，所述安全评估指令在所述服务器
接收到第三安全指数后发出，所述第三安全指数由控制端对本地安全环境评估后得到；

根据所述安全评估指令对本地环境进行安全评估，得到第一安全指数；及

15 向所述服务器发送所述第一安全指数，以触发所述服务器基于所述第一安全指数、所述第二安全指数、第三安全指数，计算门锁的安全评估结果，其中所述第二安全指数由所述服务器对指定时间段内门锁端的历史行为数据进行安全评估后得到。

相应的，本申请实施例提供一种门锁安全评估装置，包括：

20 第一发送单元，用于向门锁端发送安全评估指令，以触发所述门锁端进行本地安全环境评估，得到所述门锁端对应的第一安全指数；

获取单元，用于获取指定时间段内针对所述门锁端的历史行为数据；

第一评估单元，用于对所述历史行为数据进行安全评估分析，得到第二安全指数；

25 第一接收单元，用于接收控制端发送的第三安全指数，所述第三安全指数由所述控制端对本地安全环境评估后得到，以及接收所述门锁端发送的所述第一安全指数；

确定单元，用于基于所述第一安全指数、所述第二安全指数以及所述第三安全指数，确定门锁的安全评估结果；及

第二发送单元, 用于向所述控制端发送所述门锁的安全评估结果。

相应的, 本申请实施例提供另一种门锁安全评估装置, 包括:

第二评估单元, 用于在接收到安全评估指令时, 对本地环境进行安全评估, 得到第三安全指数;

5 第三发送单元, 用于将所述第三安全指数发送给服务器, 以触发所述服务器获取第一安全指数和第二安全指数, 其中, 所述第一安全指数由门锁端对相应的本地环境进行安全评估后得到, 所述第二安全指数由所述服务器对指定时间段内所述门锁端的历史行为数据进行安全评估后得到; 及

10 第二接收单元, 用于接收所述服务器发送的安全评估结果, 其中, 所述安全评估结果由所述服务器基于所述第一安全指数、所述第二安全指数以及所述第三安全指数计算得到。

相应的, 本申请实施例提供另一种门锁安全评估装置, 包括:

15 第三接收单元, 用于接收服务器发送的安全评估指令, 其中, 所述安全评估指令在所述服务器接收到第三安全指数后发出, 所述第三安全指数由控制端对本地安全环境评估后得到;

第三评估单元, 用于根据所述安全评估指令对本地环境进行安全评估, 得到第一安全指数; 及

20 第四发送单元, 用于向所述服务器发送所述第一安全指数, 以触发所述服务器基于所述第一安全指数、所述第二安全指数、第三安全指数, 计算门锁的安全评估结果, 其中所述第二安全指数由所述服务器对指定时间段内门锁端的历史行为数据进行安全评估后得到。

可选的, 在本申请的一些实施例中, 所述历史行为数据包括至少一个历史互动信息;

所述第一评估单元可以包括分析子单元和第一确定子单元, 如下:

25 所述分析子单元, 用于基于各个历史互动信息对应的互动时间, 对所述历史行为数据进行至少一个维度的异常分析, 得到所述至少一个维度上的异常结果; 及

第一确定子单元, 用于根据公式 $P2=100-100 * \sum_{i=1}^n D_i R_i$ 确定第二安全指数, 其中, $P2$ 表示第二安全指数, R_i 表示各个维度对应的风险系数, D_i 表示各

个维度上的异常结果，n表示维度的数量。

可选的，在本申请的一些实施例中，所述分析子单元具体可以用于对所述历史行为数据中是否存在互动时间属于预设异常时间的历史互动信息进行检测，以得到第一异常结果；或，基于各个历史互动信息对应的互动时间，对所述历史行为数据进行异常频次的分析，得到第二异常结果。

可选的，在本申请的一些实施例中，所述确定单元可以包括计算子单元和第二确定子单元，如下：

所述计算子单元，用于基于公式 $P = (P1 + P2 + P3) / 3$ ，计算门锁对应的安全评估分数，其中，P表示安全评估分数，P1表示第一安全指数，P2表示第二安全指数，P3表示第一安全指数；及

第二确定子单元，用于根据所述安全评估分数，确定所述门锁的安全评估结果。

可选的，在本申请的一些实施例中，所述第二确定子单元具体可以用于当所述安全评估分数大于预设值时，生成针对所述门锁的第一安全评估结果；当所述安全评估分数不大于预设值时，生成针对所述门锁的第二安全评估结果。

可选的，在本申请的一些实施例中，所述第二评估单元可以包括第三确定子单元、第一检测子单元和第四确定子单元，如下：

所述第三确定子单元，用于在接收到安全评估指令时，针对本地环境每个维度上的安全属性信息，确定所述维度上的安全属性信息对应的风险系数；

第一检测子单元，用于检测所述维度上的安全属性信息对应的属性值是否满足预设安全条件；及

第四确定子单元，用于基于各个维度上的安全属性信息的检测结果和风险系数，得到第三安全指数。

可选的，在本申请的一些实施例中，所述第三评估单元可以包括第五确定子单元、第二检测子单元和第六确定子单元，如下：

所述第五确定子单元，用于根据所述安全评估指令针对本地环境每个维度上的安全属性信息，确定所述维度上的安全属性信息对应的风险系数；

第二检测子单元，用于检测所述维度上的安全属性信息对应的属性值是否满足预设安全条件；及

第六确定子单元,用于基于各个维度上的安全属性信息的检测结果和风险系数,得到第一安全指数。

本申请实施例提供的一种电子设备,包括处理器和存储器,所述存储器存储有多条指令,所述处理器加载所述指令,以执行本申请实施例提供的门锁安全评估方法中的步骤。

本申请实施例还提供一种非易失性计算机可读存储介质,所述非易失性计算机可读存储介质存储有多条计算机可读指令,所述计算机可读指令适于处理器进行加载,以执行本申请实施例提供的门锁安全评估方法中的步骤。

此外,本申请实施例还提供一种计算机程序产品,包括计算机程序或计算机可读指令,该计算机程序或计算机可读指令被处理器执行时实现本申请实施例提供的门锁安全评估方法中的步骤。

本申请的一个或多个实施例的细节在下面的附图和描述中提出。本申请的其它特征和优点将从说明书、附图以及权利要求书变得明显。

附图说明

为了更清楚地说明本申请实施例中的技术方案,下面将对实施例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一些实施例,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,还可以根据这些附图获得其它的附图。。

图1a是本申请实施例提供的门锁安全评估方法的场景示意图;

图1b是本申请实施例提供的门锁安全评估方法的流程图;

图1c是本申请实施例提供的门锁安全评估方法的另一流程图;

图2a是本申请实施例提供的门锁安全评估方法的另一流程图;

图2b是本申请实施例提供的门锁安全评估方法的另一流程图;

图3a是本申请实施例提供的门锁安全评估方法的另一流程图;

图3b是本申请实施例提供的门锁安全评估方法的另一流程图;

图4a是本申请实施例提供的门锁安全评估装置的框图;

图4b是本申请实施例提供的门锁安全评估装置的框图;

图4c是本申请实施例提供的门锁安全评估装置的框图;

图 5 是本申请实施例提供的电子设备的框图。

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,本领域技术人员在没有作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。

本申请实施例提供一种门锁安全评估方法以及相关设备,相关设备可以包括门锁安全评估装置、电子设备、计算机可读存储介质和计算机程序产品。该门锁安全评估装置具体可以集成在电子设备中,该电子设备可以是终端或服务

器等设备。

如图1a所示,本申请实施例提供的门锁安全评估系统可以包括控制终端10(即门锁的控制端)、服务器11和门锁端12等;控制终端10与服务器11之间通过网络连接,门锁端12与服务器11之间也通过网络连接,比如,通过有线或无线网络连接等,其中,门锁安全评估装置可以集成在服务器中。

其中,控制终端10,可以用于:在接收到安全评估指令时,对本地环境进行安全评估,得到第三安全指数;将所述第三安全指数发送给服务器11,以触发所述服务器11获取第一安全指数和第二安全指数,其中,所述第一安全指数由门锁端12对相应的本地环境进行安全评估后得到,所述第二安全指数由所述服务器11对指定时间段内所述门锁端12的历史行为数据进行安全评估后得到;接收所述服务器11发送的安全评估结果,其中,所述安全评估结果由所述服务器11基于所述第一安全指数、所述第二安全指数以及所述第三安全指数计算得到。其中,控制终端10可以包括手机、平板电脑、电子手表、电子手环等。其中,控制终端10上还可以设置客户端,该客户端可以是应用程序客户端等等。

其中,门锁端12,可以用于:接收服务器11发送的安全评估指令,其中,所述安全评估指令在所述服务器11接收到第三安全指数后发出,所述第三安全指数由控制终端10对本地安全环境评估后得到;根据所述安全评估指令对本地环境进行安全评估,得到第一安全指数;向所述服务器11发送所述第一安全指数,以触发所述服务器11基于所述第一安全指数、所述第二安全指数、第三安

全指数，计算门锁的安全评估结果，其中所述第二安全指数由所述服务器11对指定时间段内门锁端12的历史行为数据进行安全评估后得到。

其中，服务器11，可以用于：向门锁端12发送安全评估指令，以触发所述门锁端12进行本地安全环境评估，得到所述门锁端12对应的第一安全指数；获取指定时间段内针对所述门锁端12的历史行为数据；对所述历史行为数据进行安全评估分析，得到第二安全指数；接收控制终端10发送的第三安全指数，所述第三安全指数由所述控制终端10对本地安全环境评估后得到，以及接收所述门锁端发送的所述第一安全指数；基于所述第一安全指数、所述第二安全指数以及所述第三安全指数，确定门锁的安全评估结果；向所述控制终端10发送所述门锁的安全评估结果。其中，服务器11可以是单台服务器，也可以是由多个服务器组成的服务器集群或云服务器。

上述服务器11进行门锁安全评估的步骤，也可以由控制终端10执行。

以下分别进行详细说明。需说明的是，以下实施例的描述顺序不作为对实施例优选顺序的限定。

本实施例将从第一门锁安全评估装置的角度进行描述，该第一门锁安全评估装置具体可以集成在第一电子设备中，该电子设备可以是服务器等设备。

如图1b所示，该门锁安全评估方法的具体流程可以如下：

101、向门锁端发送安全评估指令，以触发所述门锁端进行本地安全环境评估，得到所述门锁端对应的第一安全指数；

102、获取指定时间段内针对所述门锁端的历史行为数据；

103、对所述历史行为数据进行安全评估分析，得到第二安全指数；

104、接收控制端发送的第三安全指数，所述第三安全指数由所述控制端对本地安全环境评估后得到，以及接收所述门锁端发送的所述第一安全指数；

105、基于所述第一安全指数、所述第二安全指数以及所述第三安全指数，确定门锁的安全评估结果；

106、向所述控制端发送所述门锁的安全评估结果。

其中，该控制端也即门锁的控制端，门锁的控制端具体可以是能够控制开锁的电子设备，该控制端可以是手机等，本实施例对此不作限制。本实施例可以结合控制端的安全性，来确定门锁的安全性。

可选的，本实施例中，所述历史行为数据包括至少一个历史互动信息；

步骤“对所述历史行为数据进行安全评估分析，得到第二安全指数”，可以包括：

基于各个历史互动信息对应的互动时间，对所述历史行为数据进行至少一个维度的异常分析，得到所述至少一个维度上的异常结果；

根据公式 $P2 = 100 - 100 * \sum_{i=1}^n D_i R_i$ 确定第二安全指数，其中，P2表示第二安全指数， R_i 表示各个维度对应的风险系数， D_i 表示各个维度上的异常结果，n表示维度的数量。

其中，历史行为数据对应的指定时间段可以根据实际情况进行设置，如可以设置为三个月或半年等。历史行为数据具体可以是门锁的开锁数据，如开锁时间信息以及开锁是否成功等相关数据。

本实施例可以根据近期门锁开锁数据，并对其进行分析，以确定门锁的安全性。

其中，门锁的每次开锁的开锁数据可以视为一条互动信息。

其中，对历史行为数据进行至少一个维度的异常分析，可以是分析近期是否存在多次集中开锁失败、以及是否存在频繁下发一次性密码等，本实施例对此不作限制。

其中，具体地，可以根据每个维度上的异常分析对应的风险系数、以及异常结果，来确定第二安全指数，比如，以风险系数作为权重，对各个维度上的异常结果进行加权运算，得到第二安全指数。其中，对于每个维度上的异常结果，若存在异常，其异常结果可以设置为0，若没有存在异常，其异常结果可以设置为1。

可选的，本实施例中，步骤“基于各个历史互动信息对应的互动时间，对所述历史行为数据进行至少一个维度的异常分析，得到所述至少一个维度上的异常结果”，可以包括：

对所述历史行为数据中是否存在互动时间属于预设异常时间的历史互动信息进行检测，以得到第一异常结果；

或，基于各个历史互动信息对应的互动时间，对所述历史行为数据进行异常频次的分析，得到第二异常结果。

其中，该预设异常时间可以根据实际情况进行设置，本实施例不作限制，具体地，预设异常时间也可以根据各历史互动信息对应的互动时间来确定，如可以将互动时间不分布的时间段作为预设异常时间。

其中，若历史行为数据中存在互动时间属于预设异常时间的历史互动信息，则第一异常结果可以设置为0。

其中，基于各个历史互动信息对应的互动时间，对历史行为数据进行异常频次的分析，具体可以是分析近期是否存在多次集中开锁失败、是否存在频繁下发一次性密码等。若异常频次超过预设值，则第二异常结果可以设置为0。

本实施例中，用户开锁行为信息可以存储在云端，可以通过云端获取近期门锁开锁数据，并对其进行分析，如分析近期是否存在多次集中开锁失败、是否存在频繁下发一次性密码等，从而根据分析结果，计算第二安全指数P2。

在一具体实施例中，如图1c所示，展示的是云平台安全评估的流程图，具体描述如下：

1、获取近期（半年或三个月）的门锁开锁数据及门锁日志信息，并生成趋势图、异常开锁结点及相关信息；

2、分析是否有多次集中开锁失败，若近期存在多次集中开锁失败情况，则该维度上的异常结果为不通过安全检测；

3、分析是否频繁下发一次性密码，若近期存在频繁下发一次性密码情况，则该维度上的异常结果为不通过安全检测；

4、分析是否符合平时开锁行为，若近期的开锁行为存在异常，不符合平时的开锁行为，例如不符合用户平时的开锁时间，则该维度上的异常结果为不通过安全检测；

5、基于各个维度上的异常结果，计算评估分数，并生成评估结果，该评估结果即第二安全指数。

可选的，本实施例中，步骤“基于所述第一安全指数、所述第二安全指数以及所述第三安全指数，确定门锁的安全评估结果”，可以包括：

基于公式 $P = (P1 + P2 + P3) / 3$ ，计算门锁对应的安全评估分数，其中，P表示安全评估分数，P1表示第一安全指数，P2表示第二安全指数，P3表示第一安全指数；

根据所述安全评估分数，确定所述门锁的安全评估结果。

一些实施例中，不同安全评估分数可以对应不同的安全等级。比如，安全评估分数在80分以上，其安全评估结果可以是安全，若安全评估分数在60-80分，其安全评估结果可以是存在一定风险，若安全评估分数在60分以下，其安全评估结果可以是存在较大的风险。

在一具体实施例中，设智能门锁端的第一安全指数记为P1，云平台对应的第二安全指数记为P2，手机控制端对应的第三安全指数记为P3，则综合的安全评估分数 $P = (P1 + P2 + P3) / 3$ 。

具体地，如图1a所示，展示的是智能门锁安全环境评估的场景示意图，具体描述如下：

- 1、用户在手机端启动门锁对应的应用程序，点击进行智能门锁安全环境评估，可以先进行手机端的安全环境评估；
- 2、将手机端的安全评估结果传输到云平台；
- 3、云平台下发安全评估命令到智能门锁；
- 4、进行智能门锁端的安全环境评估；
- 5、将智能门锁端的安全评估结果传输到云平台；
- 6、对云平台存储的用户开锁行为进行分析，再基于云平台，手机端和智能门锁端的安全评估结果，得出门锁总体的安全评估结果；
- 7、将最终评估结果及安全建议传输给用户手机。

本申请可以通过对智能门锁对应的手机控制端，智能门锁端，云平台端的多维安全评估，能够使用户对智能门锁的安全性有清晰的认识，且基于安全评估结果，可以对用户的一些不安全的设置和行为进行提示，确保用户的安全及财产不受损失，提高了智能门锁安全性。

可选的，本实施例中，步骤“根据所述安全评估分数，确定所述门锁的安全评估结果”，可以包括：

当所述安全评估分数大于预设值时，生成针对所述门锁的第一安全评估结果；

当所述安全评估分数不大于预设值时，生成针对所述门锁的第二安全评估结果。

其中，该预设值可以根据实际情况进行设置，本实施例对此不作限制。具体地，当安全评估分数大于预设值时，可以确定第一安全评估结果为安全；当安全评估分数不大于预设值时，可以确定第二安全评估结果为存在风险。

5 由上可知，本实施例可以向门锁端发送安全评估指令，以触发所述门锁端进行本地安全环境评估，得到所述门锁端对应的第一安全指数；获取指定时间段内针对所述门锁端的历史行为数据；对所述历史行为数据进行安全评估分析，得到第二安全指数；接收控制端发送的第三安全指数，所述第三安全指数由所述控制端对本地安全环境评估后得到，以及接收所述门锁端发送的所述第一安全指数；基于所述第一安全指数、所述第二安全指数以及所述第三安全指数，
10 确定门锁的安全评估结果；向所述控制端发送所述门锁的安全评估结果。本申请可以结合门锁端、控制端以及历史行为数据三个方面，对门锁的安全性进行评估，提高了门锁对应的安全评估结果的准确性。

本实施例将从第二门锁安全评估装置的角度进行描述，该第二门锁安全评估装置具体可以集成在第二电子设备中，该第二电子设备可以是终端等设备。

15 如图2a所示，该门锁安全评估方法的具体流程如下：

201、在接收到安全评估指令时，对本地环境进行安全评估，得到第三安全指数；

202、将所述第三安全指数发送给服务器，以触发所述服务器获取第一安全指数和第二安全指数，其中，所述第一安全指数由门锁端对相应的本地环境
20 进行安全评估后得到，所述第二安全指数由所述服务器对指定时间段内所述门锁端的历史行为数据进行安全评估后得到；

203、接收所述服务器发送的安全评估结果，其中，所述安全评估结果由所述服务器基于所述第一安全指数、所述第二安全指数以及所述第三安全指数计算得到。

25 可选的，本实施例中，步骤“在接收到安全评估指令时，对本地环境进行安全评估，得到第三安全指数”，可以包括：

在接收到安全评估指令时，针对本地环境每个维度上的安全属性信息，确定所述维度上的安全属性信息对应的风险系数；

检测所述维度上的安全属性信息对应的属性值是否满足预设安全条件；

基于各个维度上的安全属性信息的检测结果和风险系数,得到第三安全指数。

其中,这里的本地环境可以是门锁的控制端对应的环境,门锁的控制端具体可以是能够控制开锁的电子设备,该控制端可以是手机等,本实施例对此不作限制。本实施例可以结合控制端的安全性,来确定门锁的安全性。

其中,每个维度上的安全属性信息可以包括控制端的系统版本、木马或漏洞、关于开锁的应用程序版本、联网环境等。

其中,每个维度上的安全属性信息对应的风险系数,具体可以是每个维度上的安全属性信息的属性值不通过预设安全条件时的风险系数,也可理解为每个维度上的安全属性信息的重要程度。

其中,每个维度上的安全属性信息的检测结果可以记为D,若该维度上的安全属性信息对应的属性值满足预设安全条件,则该维度上的安全属性信息可以视为通过了安全检测,将其检测结果D设置为1;若该维度上的安全属性信息对应的属性值不满足预设安全条件,则该维度上的安全属性信息可以视为不通过安全检测,将其检测结果D设置为0。

其中,预设安全条件可以根据实际情况进行设置,本实施例对此不作限制。比如,若某个维度上的安全属性信息为手机系统版本,其属性值可以是版本号,则预设安全条件可以是手机系统版本不低于最新发布版本。又比如,某个维度上的安全属性信息为系统木马或漏洞,其属性值可以是系统是否存在木马或漏洞,预设安全条件可以是系统没有存在木马或漏洞。

其中,步骤“基于各个维度上的安全属性信息的检测结果和风险系数,得到第三安全指数”,可以包括:

将各个维度上的安全属性信息的风险系数作为权重;

基于所述权重,对各个维度上的安全属性信息的检测结果进行加权运算,得到所述控制端对应的第三安全指数。

可以理解的是,也可以通过其他方式来获取第三安全指数本实施例对此不作限制。

在一具体场景中,门锁对应的控制端可以是手机端,对于手机端,可以先确定其安全评估检测项目数n,也即安全属性信息的维度数量,比如,安全评

估检测项目（即各个维度上的安全属性信息）可以包括：手机系统版本、木马或漏洞检测、应用程序版本、手机联网环境等，若每个安全评估检测项目的检测结果记为 D_i ，风险系数记为 R_i ，第三安全指数记为 $P3$ ，则手机端对应的第三安全指数可以为 $P3 = 100 - 100 * \sum_{i=1}^n D_i R_i$ ；其中，各安全评估检测项目的风险系数之和可以为1。

如图2b所示，展示的是手机端安全评估的流程图，具体描述如下：

1、对手机系统版本进行检测，若版本低于最新发布版本，则该维度上的安全属性信息不通过安全检测；

2、对手机系统木马或漏洞进行检测，若发现木马或严重漏洞，则该维度上的安全属性信息不通过安全检测；

3、对手机系统安全设置检测，若手机未开启SELinux（Security-Enhanced Linux，安全增强型Linux）或进入开发者模式，则该维度上的安全属性信息不通过安全检测；其中，Linux是一种操作系统；

4、对手机联网环境进行检测，若手机连接的是无密码网络，则该维度上的安全属性信息不通过安全检测；

5、对手机应用程序的版本进行检测，若版本低于最新发布版本，则该维度上的安全属性信息不通过安全检测；

6、对手机应用程序的设置进行检测，若用户密码设置简单或很久没有更改密码，则该维度上的安全属性信息不通过安全检测；

7、基于各个维度上的安全属性信息的检测结果，计算评估分数，并生成评估结果，该评估结果即为控制端的第三安全指数。

由上可知，本实施例可以在接收到安全评估指令时，对本地环境进行安全评估，得到第三安全指数；将所述第三安全指数发送给服务器，以触发所述服务器获取第一安全指数和第二安全指数，其中，所述第一安全指数由门锁端对相应的本地环境进行安全评估后得到，所述第二安全指数由所述服务器对指定时间段内所述门锁端的历史行为数据进行安全评估后得到；接收所述服务器发送的安全评估结果，其中，所述安全评估结果由所述服务器基于所述第一安全指数、所述第二安全指数以及所述第三安全指数计算得到。本申请可以结合门锁端、控制端以及历史行为数据三个方面，对门锁的安全性进行评估，提高了

门锁对应的安全评估结果的准确性。

本实施例将从第三门锁安全评估装置的角度进行描述，该第三门锁安全评估装置具体可以集成在第三电子设备中，该第三电子设备可以为门锁端对应的设备。

5 如图3a所示，该门锁安全评估方法的具体流程如下：

301、接收服务器发送的安全评估指令，其中，所述安全评估指令在所述服务器接收到第三安全指数后发出，所述第三安全指数由控制端对本地安全环境评估后得到；

10 302、根据所述安全评估指令对本地环境进行安全评估，得到第一安全指数；

303、向所述服务器发送所述第一安全指数，以触发所述服务器基于所述第一安全指数、所述第二安全指数、第三安全指数，计算门锁的安全评估结果，其中所述第二安全指数由所述服务器对指定时间段内门锁端的历史行为数据进行安全评估后得到。

15 可选的，本实施例中，步骤“根据所述安全评估指令对本地环境进行安全评估，得到第一安全指数”，可以包括：

根据所述安全评估指令针对本地环境每个维度上的安全属性信息，确定所述维度上的安全属性信息对应的风险系数；

检测所述维度上的安全属性信息对应的属性值是否满足预设安全条件；

20 基于各个维度上的安全属性信息的检测结果和风险系数，得到第一安全指数。

其中，这里的本地环境具体指门锁端对应的环境，门锁端在各个维度上的安全属性信息可以包括MCU（微控制单元，Microcontroller Unit）模块固件版本信息、WiFi（无线通信技术）模块固件版本信息、指纹模块固定版本信息等。

25 其中，每个维度上的安全属性信息的检测结果可以记为D，若该维度上的安全属性信息对应的属性值满足预设安全条件，则该维度上的安全属性信息可以视为通过了安全检测，将其检测结果D设置为1；若该维度上的安全属性信息对应的属性值不满足预设安全条件，则该维度上的安全属性信息可以视为不通过安全检测，将其检测结果D设置为0。

其中,预设安全条件可以根据实际情况进行设置,本实施例对此不作限制。比如,若某个维度上的安全属性信息为手MCU模块固件版本信息,其属性值可以是版本号,则预设安全条件可以是MCU模块固件版本不低于其最新发布版本。又比如,某个维度上的安全属性信息为指纹模块固定版本信息,其属性值可以是版本号,预设安全条件可以是指纹模块固定版本不低于其最新发布版本。

其中,步骤“基于各个维度上的安全属性信息的检测结果和风险系数,得到第一安全指数”,可以包括:

将各个维度上的安全属性信息的风险系数作为权重;

基于所述权重,对各个维度上的安全属性信息的检测结果进行加权运算,得到第一安全指数。

可以理解的是,也可以通过其他方式来获取第一安全指数本实施例对此不作限制。

在一具体场景中,对于智能门锁端,同样确定其安全评估检测项目数 n ,也即门锁端的安全属性信息的维度数量,比如,安全评估检测项目(即各个维度上的安全属性信息)可以包括:MCU模块固件版本信息、WiFi模块固件版本信息、指纹模块固定版本信息等,若每个安全评估检测项目的检测结果记为 D_i ,风险系数记为 R_i ,第一安全指数记为 $P1$,则智能门锁端对应的第一安全指数可以为 $P1 = 100 - 100 * \sum_{i=1}^n D_i R_i$;其中,各安全评估检测项目的风险系数之和可以为1。

如图3b所示,展示的是智能门锁端安全评估的流程图,具体描述如下:

1、检测MCU(微控制单元)模块固件版本信息,若版本低于最新发布版本,则该维度上的安全属性信息不通过安全检测;

2、检测WiFi(无线网络)模块固件版本信息,若版本低于最新发布版本,则该维度上的安全属性信息不通过安全检测;

3、检测指纹模块固件版本信息,若版本低于最新发布版本,则该维度上的安全属性信息不通过安全检测;

4、检测人脸模块固件版本信息,若版本低于最新发布版本,则该维度上的安全属性信息不通过安全检测;

5、检测猫眼模块固件版本信息，若版本低于最新发布版本，则该维度上的安全属性信息不通过安全检测；

6、基于各个维度上的安全属性信息的检测结果，计算评估分数，并生成评估结果，该评估结果即为门锁端的第一安全指数。

5 本申请可以通过对智能门锁对应的手机控制端，智能门锁端，云平台端的多维安全评估，能够使用户对智能门锁的安全性有清晰的认识，且基于安全评估结果，可以对用户的一些不安全的设置和行为进行提示，确保用户的安全及财产不受损失，提高了智能门锁安全性。

10 由上可知，本实施例可以接收服务器发送的安全评估指令，其中，所述安全评估指令在所述服务器接收到第三安全指数后发出，所述第三安全指数由控制端对本地安全环境评估后得到；根据所述安全评估指令对本地环境进行安全评估，得到第一安全指数；向所述服务器发送所述第一安全指数，以触发所述服务器基于所述第一安全指数、所述第二安全指数、第三安全指数，计算门锁的安全评估结果，其中所述第二安全指数由所述服务器对指定时间段内门锁端的历史行为数据进行安全评估后得到。本申请可以结合门锁端、控制端以及历史行为数据三个方面，对门锁的安全性进行评估，提高了门锁对应的安全评估结果的准确性。

为了更好地实施以上方法，本申请实施例还提供一种门锁安全评估系统，该门锁安全评估系统包括第一门锁安全评估装置 41、第二门锁安全评估装置 20 42 和第三门锁安全评估装置 43，其中，第一门锁安全评估装置 41 具体可以集成在服务器中，第二门锁安全评估装置 42 可以视为门锁的控制终端，第三门锁安全评估装置 43 可以视为门锁端。如图 4a 所示，该第一门锁安全评估装置 41 可以包括第一发送单元 4101、获取单元 4102、第一评估单元 4103、第一接收单元 4104、确定单元 4105、以及第二发送单元 4106；如图 4b 所示，第二门锁安全评估装置 42 可以包括第二评估单元 4201、第三发送单元 4202 以及第二接收单元 4203；如图 4c 所示，第三门锁安全评估装置 43 可以包括第三接收单元 4301、第三评估单元 4302 以及第四发送单元 4303，如下：

A、第一门锁安全评估装置41

(1) 第一发送单元4101；

第一发送单元,用于向门锁端发送安全评估指令,以触发所述门锁端进行本地安全环境评估,得到所述门锁端对应的第一安全指数。

(2) 获取单元4102;

获取单元,用于获取指定时间段内针对所述门锁端的历史行为数据。

5 (3) 第一评估单元4103;

第一评估单元,用于对所述历史行为数据进行安全评估分析,得到第二安全指数。

可选的,在本申请的一些实施例中,所述历史行为数据包括至少一个历史互动信息;

10 所述第一评估单元可以包括分析子单元和第一确定子单元,如下:

所述分析子单元,用于基于各个历史互动信息对应的互动时间,对所述历史行为数据进行至少一个维度的异常分析,得到所述至少一个维度上的异常结果;

15 第一确定子单元,用于根据公式 $P2=100-100*\sum_{i=1}^n D_i R_i$ 确定第二安全指数,其中,P2表示第二安全指数, R_i 表示各个维度对应的风险系数, D_i 表示各个维度上的异常结果,n表示维度的数量。

20 可选的,在本申请的一些实施例中,所述分析子单元具体可以用于对所述历史行为数据中是否存在互动时间属于预设异常时间的历史互动信息进行检测,以得到第一异常结果;或,基于各个历史互动信息对应的互动时间,对所述历史行为数据进行异常频次的分析,得到第二异常结果。

(4) 第一接收单元4104;

第一接收单元,用于接收控制端发送的第三安全指数,所述第三安全指数由所述控制端对本地安全环境评估后得到,以及接收所述门锁端发送的所述第一安全指数。

25 (5) 确定单元4105;

确定单元,用于基于所述第一安全指数、所述第二安全指数以及所述第三安全指数,确定门锁的安全评估结果。

可选的,在本申请的一些实施例中,所述确定单元可以包括计算子单元和第二确定子单元,如下:

所述计算子单元, 用于基于公式 $P = (P1 + P2 + P3) / 3$, 计算门锁对应的安全评估分数, 其中, P 表示安全评估分数, $P1$ 表示第一安全指数, $P2$ 表示第二安全指数, $P3$ 表示第一安全指数;

5 第二确定子单元, 用于根据所述安全评估分数, 确定所述门锁的安全评估结果。

可选的, 在本申请的一些实施例中, 所述第二确定子单元具体可以用于当所述安全评估分数大于预设值时, 生成针对所述门锁的第一安全评估结果; 当所述安全评估分数不大于预设值时, 生成针对所述门锁的第二安全评估结果。

(6) 第二发送单元4106;

10 第二发送单元, 用于向所述控制端发送所述门锁的安全评估结果。

B、第二门锁安全评估装置42

(7) 第二评估单元4201;

第二评估单元, 用于在接收到安全评估指令时, 对本地环境进行安全评估, 得到第三安全指数。

15 可选的, 在本申请的一些实施例中, 所述第二评估单元可以包括第三确定子单元、第一检测子单元和第四确定子单元, 如下:

所述第三确定子单元, 用于在接收到安全评估指令时, 针对本地环境每个维度上的安全属性信息, 确定所述维度上的安全属性信息对应的风险系数;

20 第一检测子单元, 用于检测所述维度上的安全属性信息对应的属性值是否满足预设安全条件;

第四确定子单元, 用于基于各个维度上的安全属性信息的检测结果和风险系数, 得到第三安全指数。

(8) 第三发送单元4202;

25 第三发送单元, 用于将所述第三安全指数发送给服务器, 以触发所述服务器获取第一安全指数和第二安全指数, 其中, 所述第一安全指数由门锁端对相应的本地环境进行安全评估后得到, 所述第二安全指数由所述服务器对指定时间段内所述门锁端的历史行为数据进行安全评估后得到。

(9) 第二接收单元4203;

第二接收单元, 用于接收所述服务器发送的安全评估结果, 其中, 所述安

全评估结果由所述服务器基于所述第一安全指数、所述第二安全指数以及所述第三安全指数计算得到。

C、第三门锁安全评估装置43

(10) 第三接收单元4301;

5 第三接收单元, 用于接收服务器发送的安全评估指令, 其中, 所述安全评估指令在所述服务器接收到第三安全指数后发出, 所述第三安全指数由控制端对本地安全环境评估后得到。

(11) 第三评估单元4302;

10 第三评估单元, 用于根据所述安全评估指令对本地环境进行安全评估, 得到第一安全指数。

可选的, 在本申请的一些实施例中, 所述第三评估单元可以包括第五确定子单元、第二检测子单元和第六确定子单元, 如下:

所述第五确定子单元, 用于根据所述安全评估指令针对本地环境每个维度上的安全属性信息, 确定所述维度上的安全属性信息对应的风险系数;

15 第二检测子单元, 用于检测所述维度上的安全属性信息对应的属性值是否满足预设安全条件;

第六确定子单元, 用于基于各个维度上的安全属性信息的检测结果和风险系数, 得到第一安全指数。

(12) 第四发送单元4303;

20 第四发送单元, 用于向所述服务器发送所述第一安全指数, 以触发所述服务器基于所述第一安全指数、所述第二安全指数、第三安全指数, 计算门锁的安全评估结果, 其中所述第二安全指数由所述服务器对指定时间段内门锁端的历史行为数据进行安全评估后得到。

25 由上可知, 本实施例可以通过第一发送单元4101向门锁端发送安全评估指令, 以触发所述门锁端进行本地安全环境评估, 得到所述门锁端对应的第一安全指数; 由获取单元4102获取指定时间段内针对所述门锁端的历史行为数据; 通过第一评估单元4103对所述历史行为数据进行安全评估分析, 得到第二安全指数; 由第一接收单元4104接收控制端发送的第三安全指数, 所述第三安全指数由所述控制端对本地安全环境评估后得到, 以及接收所述门锁端发送的所述

第一安全指数；通过确定单元4105基于所述第一安全指数、所述第二安全指数以及所述第三安全指数，确定门锁的安全评估结果；由第二发送单元4106向所述控制端发送所述门锁的安全评估结果；

5 或者，在接收到安全评估指令时，通过第二评估单元4201对本地环境进行安全评估，得到第三安全指数；通过第三发送单元4202将所述第三安全指数发送给服务器，以触发所述服务器获取第一安全指数和第二安全指数，其中，所述第一安全指数由门锁端对相应的本地环境进行安全评估后得到，所述第二安全指数由所述服务器对指定时间段内所述门锁端的历史行为数据进行安全评估后得到；通过第二接收单元4203接收所述服务器发送的安全评估结果，其中，
10 所述安全评估结果由所述服务器基于所述第一安全指数、所述第二安全指数以及所述第三安全指数计算得到；

或者，由第三接收单元4301接收服务器发送的安全评估指令，其中，所述安全评估指令在所述服务器接收到第三安全指数后发出，所述第三安全指数由控制端对本地安全环境评估后得到；通过第三评估单元4302根据所述安全评估
15 指令对本地环境进行安全评估，得到第一安全指数；通过第四发送单元4303向所述服务器发送所述第一安全指数，以触发所述服务器基于所述第一安全指数、所述第二安全指数、第三安全指数，计算门锁的安全评估结果，其中所述第二安全指数由所述服务器对指定时间段内门锁端的历史行为数据进行安全评估后得到；

20 本申请可以结合门锁端、门锁的控制端以及历史行为数据三个方面，对门锁的安全性进行评估，提高了门锁对应的安全评估结果的准确性。

本申请实施例还提供一种电子设备，如图5所示，其示出了本申请实施例所涉及的电子设备的结构示意图，该电子设备可以是终端或者服务器等，具体来讲：

25 该电子设备可以包括一个或者一个以上处理核心的处理器501、一个或一个以上计算机可读存储介质的存储器502、电源503和输入单元504等部件。本领域技术人员可以理解，图5中示出的电子设备结构并不构成对电子设备的限定，可以包括比图示更多或更少的部件，或者组合某些部件，或者不同的部件布置。其中：

处理器 501 是该电子设备的控制中心, 利用各种接口和线路连接整个电子设备的各个部分, 通过运行或执行存储在存储器 502 内的软件程序和/或模块, 以及调用存储在存储器 502 内的数据, 执行电子设备的各种功能和处理数据, 从而对电子设备进行整体监控。可选的, 处理器 501 可包括一个或多个处理核
5 心; 优选的, 处理器 501 可集成应用处理器和调制解调处理器, 其中, 应用处理器主要处理操作系统、用户界面和应用程序等, 调制解调处理器主要处理无线通信。可以理解的是, 上述调制解调处理器也可以不集成到处理器 501 中。

存储器 502 可用于存储软件程序以及模块, 处理器 501 通过运行存储在存储器 502 的软件程序以及模块, 从而执行各种功能应用以及数据处理。存储器
10 502 可主要包括存储程序区和存储数据区, 其中, 存储程序区可存储操作系统、至少一个功能所需的应用程序 (比如声音播放功能、图像播放功能等) 等; 存储数据区可存储根据电子设备的使用所创建的数据等。此外, 存储器 502 可以包括高速随机存取存储器, 还可以包括非易失性存储器, 例如至少一个磁盘存储器件、闪存器件、或其他易失性固态存储器件。相应地, 存储器 502 还可以
15 包括存储器控制器, 以提供处理器 501 对存储器 502 的访问。

电子设备还包括给各个部件供电的电源 503, 优选的, 电源 503 可以通过电源管理系统与处理器 501 逻辑相连, 从而通过电源管理系统实现管理充电、放电、以及功耗管理等功能。电源 503 还可以包括一个或一个以上的直流或交流电源、再充电系统、电源故障检测电路、电源转换器或者逆变器、电源状态
20 指示器等任意组件。

该电子设备还可包括输入单元 504, 该输入单元 504 可用于接收输入的数字或字符信息, 以及产生与用户设置以及功能控制有关的键盘、鼠标、操作杆、光学或者轨迹球信号输入。

尽管未示出, 该电子设备还可以包括显示单元等, 在此不再赘述。具体在
25 本实施例中, 电子设备中的处理器 501 会按照如下的指令, 将一个或一个以上的应用程序的进程对应的可执行文件加载到存储器 502 中, 并由处理器 501 来运行存储在存储器 502 中的应用程序, 从而实现各种功能, 如下:

向门锁端发送安全评估指令, 以触发所述门锁端进行本地安全环境评估, 得到所述门锁端对应的第一安全指数; 获取指定时间段内针对所述门锁端的历

史行为数据；对所述历史行为数据进行安全评估分析，得到第二安全指数；接收控制端发送的第三安全指数，所述第三安全指数由所述控制端对本地安全环境评估后得到，以及接收所述门锁端发送的所述第一安全指数；基于所述第一安全指数、所述第二安全指数以及所述第三安全指数，确定门锁的安全评估结果；

5 向所述控制端发送所述门锁的安全评估结果；

或者，

在接收到安全评估指令时，对本地环境进行安全评估，得到第三安全指数；将所述第三安全指数发送给服务器，以触发所述服务器获取第一安全指数和第二安全指数，其中，所述第一安全指数由门锁端对相应的本地环境进行安全评估后得到，所述第二安全指数由所述服务器对指定时间段内所述门锁端的历史行为数据进行安全评估后得到；接收所述服务器发送的安全评估结果，其中，所述安全评估结果由所述服务器基于所述第一安全指数、所述第二安全指数以及所述第三安全指数计算得到；

10

或者，

接收服务器发送的安全评估指令，其中，所述安全评估指令在所述服务器接收到第三安全指数后发出，所述第三安全指数由控制端对本地安全环境评估后得到；根据所述安全评估指令对本地环境进行安全评估，得到第一安全指数；向所述服务器发送所述第一安全指数，以触发所述服务器基于所述第一安全指数、所述第二安全指数、第三安全指数，计算门锁的安全评估结果，其中所述

15

20 第二安全指数由所述服务器对指定时间段内门锁端的历史行为数据进行安全评估后得到。

以上各个操作的具体实施可参见前面的实施例，在此不再赘述。

由上可知，本实施例可以向门锁端发送安全评估指令，以触发所述门锁端进行本地安全环境评估，得到所述门锁端对应的第一安全指数；获取指定时间段内针对所述门锁端的历史行为数据；对所述历史行为数据进行安全评估分析，得到第二安全指数；接收控制端发送的第三安全指数，所述第三安全指数由所述控制端对本地安全环境评估后得到，以及接收所述门锁端发送的所述第一安全指数；基于所述第一安全指数、所述第二安全指数以及所述第三安全指数，确定门锁的安全评估结果；向所述控制端发送所述门锁的安全评估结果。

25

本申请可以结合门锁端、控制端以及历史行为数据三个方面，对门锁的安全性进行评估，提高了门锁对应的安全评估结果的准确性。

本领域普通技术人员可以理解，上述实施例的各种方法中的全部或部分步骤可以通过计算机可读指令来完成，或通过计算机可读指令控制相关的硬件来完成，该计算机可读指令可以存储于一计算机可读存储介质中，并由处理器进行加载和执行。

为此，本申请实施例提供一种非易失性计算机可读存储介质，其中存储有多条计算机可读指令，该计算机可读指令能够被处理器进行加载，以执行本申请实施例所提供的任一种门锁安全评估方法中的步骤。例如，该计算机可读指令可以执行如下步骤：

向门锁端发送安全评估指令，以触发所述门锁端进行本地安全环境评估，得到所述门锁端对应的第一安全指数；获取指定时间段内针对所述门锁端的历史行为数据；对所述历史行为数据进行安全评估分析，得到第二安全指数；接收控制端发送的第三安全指数，所述第三安全指数由所述控制端对本地安全环境评估后得到，以及接收所述门锁端发送的所述第一安全指数；基于所述第一安全指数、所述第二安全指数以及所述第三安全指数，确定门锁的安全评估结果；向所述控制端发送所述门锁的安全评估结果；

或者，

在接收到安全评估指令时，对本地环境进行安全评估，得到第三安全指数；将所述第三安全指数发送给服务器，以触发所述服务器获取第一安全指数和第二安全指数，其中，所述第一安全指数由门锁端对相应的本地环境进行安全评估后得到，所述第二安全指数由所述服务器对指定时间段内所述门锁端的历史行为数据进行安全评估后得到；接收所述服务器发送的安全评估结果，其中，所述安全评估结果由所述服务器基于所述第一安全指数、所述第二安全指数以及所述第三安全指数计算得到；

或者，

接收服务器发送的安全评估指令，其中，所述安全评估指令在所述服务器接收到第三安全指数后发出，所述第三安全指数由控制端对本地安全环境评估后得到；根据所述安全评估指令对本地环境进行安全评估，得到第一安全指数；

向所述服务器发送所述第一安全指数，以触发所述服务器基于所述第一安全指数、所述第二安全指数、第三安全指数，计算门锁的安全评估结果，其中所述第二安全指数由所述服务器对指定时间段内门锁端的历史行为数据进行安全评估后得到。

5 以上各个操作的具体实施可参见前面的实施例，在此不再赘述。

其中，该非易失性计算机可读存储介质可以包括：只读存储器（ROM，Read Only Memory）、随机存取记忆体（RAM，Random Access Memory）、磁盘或光盘等。

10 由于该非易失性计算机可读存储介质中所存储的指令，可以执行本申请实施例所提供的任一种门锁安全评估方法中的步骤，因此，可以实现本申请实施例所提供的任一种门锁安全评估方法所能实现的有益效果，详见前面的实施例，在此不再赘述。

15 根据本申请的一个方面，提供了一种计算机程序产品或计算机程序，该计算机程序产品或计算机程序包括计算机可读指令，该计算机可读指令存储在非易失性计算机可读存储介质中。计算机设备的处理器从非易失性计算机可读存储介质读取该计算机可读指令，处理器执行该计算机可读指令，使得该计算机设备执行上述门锁安全评估方面的各种可选实现方式中提供的方法。

20 以上对本申请实施例所提供的一种门锁安全评估方法以及相关设备进行了详细介绍，本文中应用了具体个例对本申请的原理及实施方式进行了阐述，以上实施例的说明只是用于帮助理解本申请的方法及其核心思想；同时，对于本领域的技术人员，依据本申请的思想，在具体实施方式及应用范围上均会有改变之处，综上所述，本说明书内容不应理解为对本申请的限制。

权 利 要 求 书

1、一种门锁安全评估方法，其特征在于，包括：

向门锁端发送安全评估指令，以触发所述门锁端进行本地安全环境评估，得到所述门锁端对应的第一安全指数；

5 获取指定时间段内针对所述门锁端的历史行为数据；

对所述历史行为数据进行安全评估分析，得到第二安全指数；

接收控制端发送的第三安全指数，所述第三安全指数由所述控制端对本地安全环境评估后得到，以及接收所述门锁端发送的所述第一安全指数；

10 基于所述第一安全指数、所述第二安全指数以及所述第三安全指数，确定门锁的安全评估结果；及

向所述控制端发送所述门锁的安全评估结果。

2、根据权利要求1所述的方法，其特征在于，所述历史行为数据包括至少一个历史互动信息；

所述对所述历史行为数据进行安全评估分析，得到第二安全指数，包括：

15 基于各个历史互动信息对应的互动时间，对所述历史行为数据进行至少一个维度的异常分析，得到所述至少一个维度上的异常结果；及

根据公式 $P2=100-100*\sum_{i=1}^n D_i R_i$ 确定第二安全指数，其中，P2表示第二安全指数， R_i 表示各个维度对应的风险系数， D_i 表示各个维度上的异常结果，n表示维度的数量。

20 3、根据权利要求2所述的方法，其特征在于，所述基于各个历史互动信息对应的互动时间，对所述历史行为数据进行至少一个维度的异常分析，得到所述至少一个维度上的异常结果，包括：

对所述历史行为数据中是否存在互动时间属于预设异常时间的历史互动信息进行检测，以得到第一异常结果；

25 或，基于各个历史互动信息对应的互动时间，对所述历史行为数据进行异常频次的分析，得到第二异常结果。

4、根据权利要求1所述的方法，其特征在于，所述基于所述第一安全指数、所述第二安全指数以及所述第三安全指数，确定门锁的安全评估结果，包括：

基于公式 $P = (P1 + P2 + P3) / 3$ ，计算门锁对应的安全评估分数，其中，P表示安全评估分数，P1表示第一安全指数，P2表示第二安全指数，P3表示第一安全指数；及

根据所述安全评估分数，确定所述门锁的安全评估结果。

5 5、根据权利要求4所述的方法，其特征在于，所述根据所述安全评估分数，确定所述门锁的安全评估结果，包括：

当所述安全评估分数大于预设值时，生成针对所述门锁的第一安全评估结果；及

10 当所述安全评估分数不大于预设值时，生成针对所述门锁的第二安全评估结果。

6、一种门锁安全评估方法，其特征在于，包括：

在接收到安全评估指令时，对本地环境进行安全评估，得到第三安全指数；

15 将所述第三安全指数发送给服务器，以触发所述服务器获取第一安全指数和第二安全指数，其中，所述第一安全指数由门锁端对相应的本地环境进行安全评估后得到，所述第二安全指数由所述服务器对指定时间段内所述门锁端的历史行为数据进行安全评估后得到；及

接收所述服务器发送的安全评估结果，其中，所述安全评估结果由所述服务器基于所述第一安全指数、所述第二安全指数以及所述第三安全指数计算得到。

20 7、根据权利要求6所述的方法，其特征在于，所述在接收到安全评估指令时，对本地环境进行安全评估，得到第三安全指数，包括：

在接收到安全评估指令时，针对本地环境每个维度上的安全属性信息，确定所述维度上的安全属性信息对应的风险系数；

检测所述维度上的安全属性信息对应的属性值是否满足预设安全条件；及

25 基于各个维度上的安全属性信息的检测结果和风险系数，得到第三安全指数。

8、根据权利要求7所述的方法，其特征在于，所述基于各个维度上的安全属性信息的检测结果和风险系数，得到第三安全指数，包括：

将各个维度上的安全属性信息的风险系数作为权重；及

基于所述权重，对各个维度上的安全属性信息的检测结果进行加权运算，得到所述控制端对应的第三安全指数。

9、一种门锁安全评估方法，其特征在于，包括：

接收服务器发送的安全评估指令，其中，所述安全评估指令在所述服务器
5 接收到第三安全指数后发出，所述第三安全指数由控制端对本地安全环境评估后得到；

根据所述安全评估指令对本地环境进行安全评估，得到第一安全指数；及

向所述服务器发送所述第一安全指数，以触发所述服务器基于所述第一安全指数、所述第二安全指数、第三安全指数，计算门锁的安全评估结果，其中
10 所述第二安全指数由所述服务器对指定时间段内门锁端的历史行为数据进行安全评估后得到。

10、根据权利要求9所述的方法，其特征在于，所述根据所述安全评估指令对本地环境进行安全评估，得到第一安全指数，包括：

根据所述安全评估指令针对本地环境每个维度上的安全属性信息，确定所
15 述维度上的安全属性信息对应的风险系数；

检测所述维度上的安全属性信息对应的属性值是否满足预设安全条件；及

基于各个维度上的安全属性信息的检测结果和风险系数，得到第一安全指数。

11、根据权利要求9所述的方法，其特征在于，所述基于各个维度上的安全属性信息的检测结果和风险系数，得到第一安全指数，包括：
20 将各个维度上的安全属性信息的风险系数作为权重；及

基于所述权重，对各个维度上的安全属性信息的检测结果进行加权运算，

得到第一安全指数。

12、一种门锁安全评估装置，其特征在于，包括：

25 第一发送单元，用于向门锁端发送安全评估指令，以触发所述门锁端进行本地安全环境评估，得到所述门锁端对应的第一安全指数；

获取单元，用于获取指定时间段内针对所述门锁端的历史行为数据；

第一评估单元，用于对所述历史行为数据进行安全评估分析，得到第二安全指数；

第一接收单元,用于接收控制端发送的第三安全指数,所述第三安全指数由所述控制端对本地安全环境评估后得到,以及接收所述门锁端发送的所述第一安全指数;

5 确定单元,用于基于所述第一安全指数、所述第二安全指数以及所述第三安全指数,确定门锁的安全评估结果;及

第二发送单元,用于向所述控制端发送所述门锁的安全评估结果。

13、一种门锁安全评估装置,其特征在于,包括:

第二评估单元,用于在接收到安全评估指令时,对本地环境进行安全评估,得到第三安全指数;

10 第三发送单元,用于将所述第三安全指数发送给服务器,以触发所述服务器获取第一安全指数和第二安全指数,其中,所述第一安全指数由门锁端对相应的本地环境进行安全评估后得到,所述第二安全指数由所述服务器对指定时间段内所述门锁端的历史行为数据进行安全评估后得到;及

15 第二接收单元,用于接收所述服务器发送的安全评估结果,其中,所述安全评估结果由所述服务器基于所述第一安全指数、所述第二安全指数以及所述第三安全指数计算得到。

14、一种门锁安全评估装置,其特征在于,包括:

20 第三接收单元,用于接收服务器发送的安全评估指令,其中,所述安全评估指令在所述服务器接收到第三安全指数后发出,所述第三安全指数由控制端对本地安全环境评估后得到;

第三评估单元,用于根据所述安全评估指令对本地环境进行安全评估,得到第一安全指数;及

25 第四发送单元,用于向所述服务器发送所述第一安全指数,以触发所述服务器基于所述第一安全指数、所述第二安全指数、第三安全指数,计算门锁的安全评估结果,其中所述第二安全指数由所述服务器对指定时间段内门锁端的历史行为数据进行安全评估后得到。

15、一种电子设备,其特征在于,包括存储器和处理器;所述存储器存储有应用程序,所述处理器用于运行所述存储器内的应用程序,以执行权利要求1至11任一项所述的门锁安全评估方法中的操作。

16、一种非易失性计算机可读存储介质，其特征在于，所述非易失性计算机可读存储介质存储有多条计算机可读指令，所述计算机可读指令适于处理器进行加载，以执行权利要求 1 至 11 任一项所述的门锁安全评估方法中的步骤。

5 17、一种计算机程序产品，包括计算机程序或计算机可读指令，其特征在于，该计算机程序或计算机可读指令被处理器执行时实现权利要求 1 至 11 任一项所述的门锁安全评估方法中的步骤。

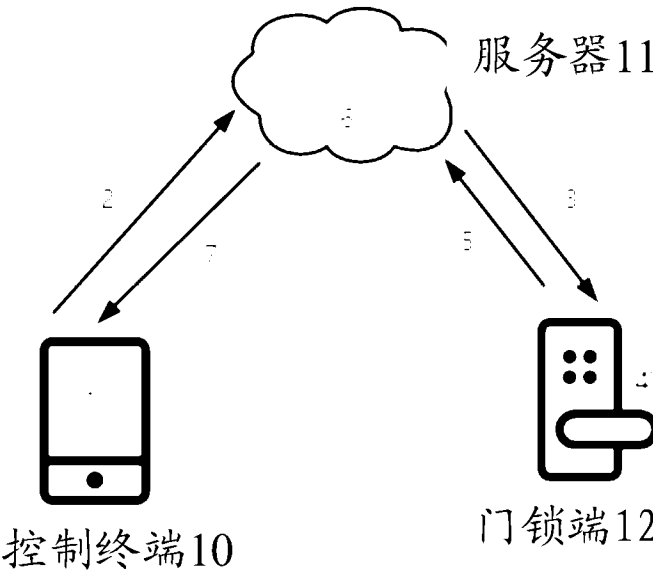


图 1a

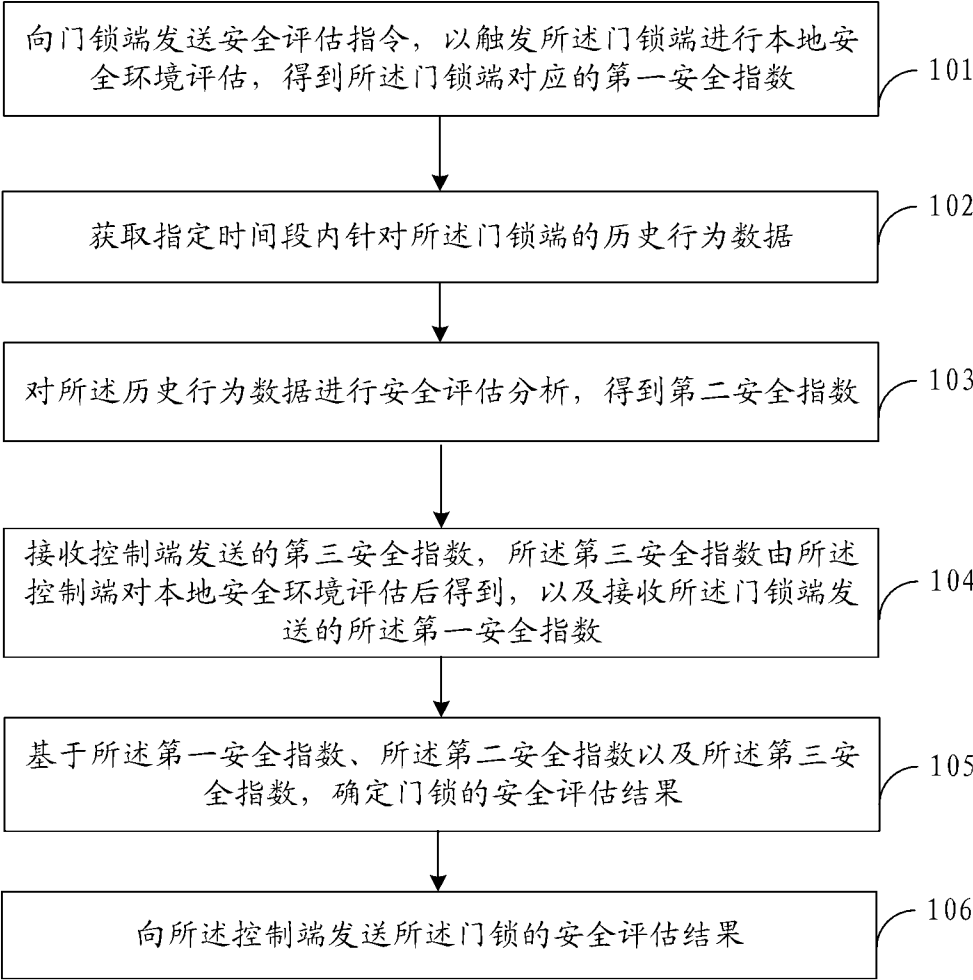


图 1b

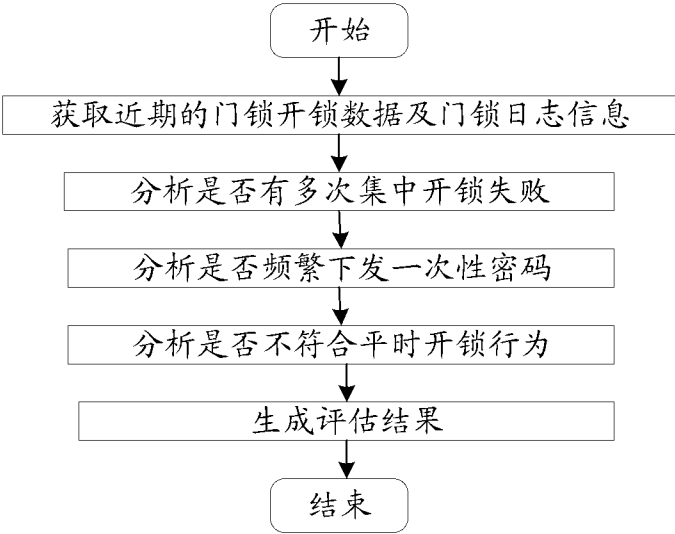


图 1c

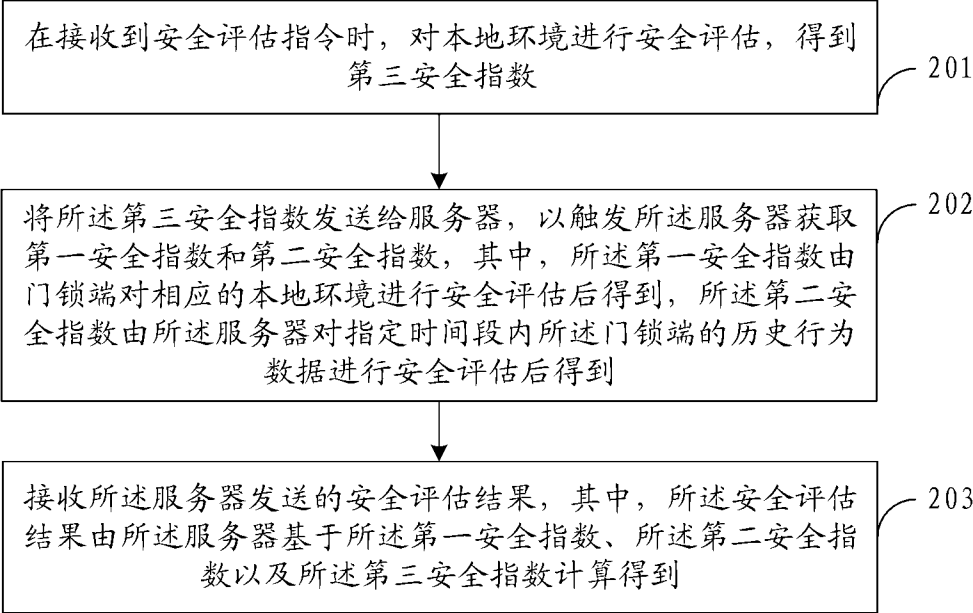


图 2a

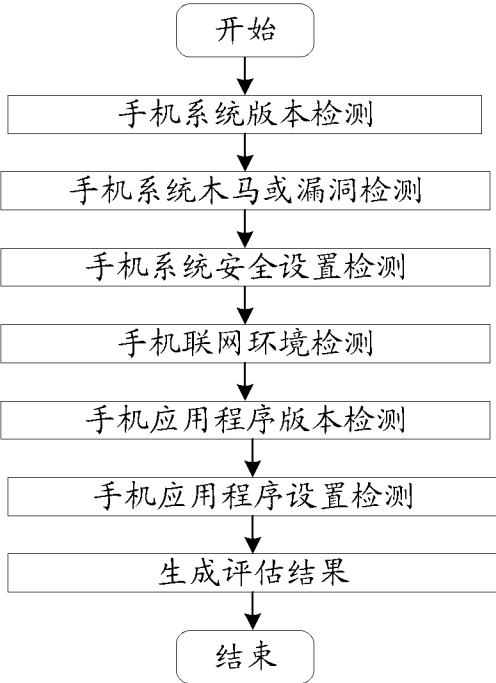


图 2b

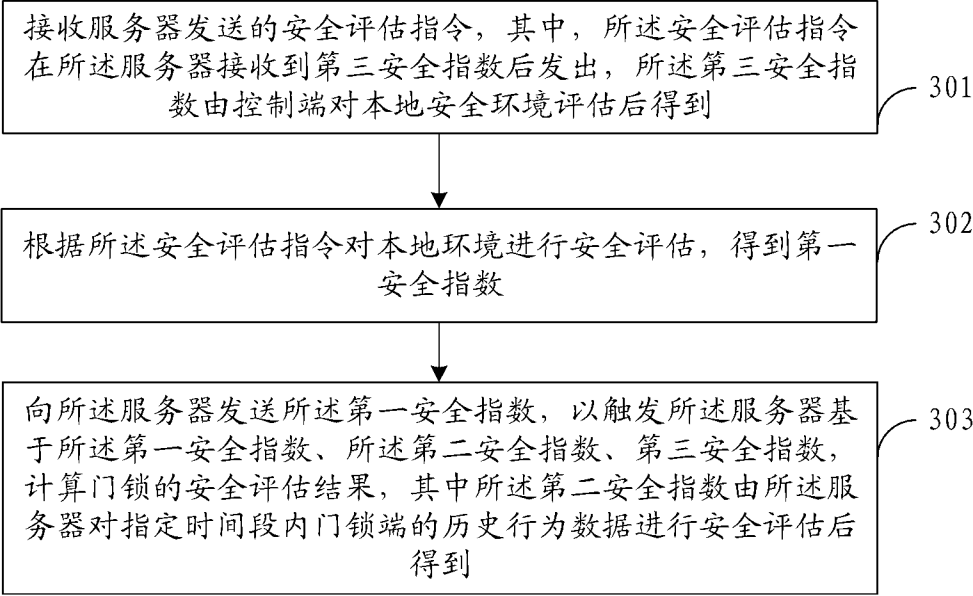


图 3a

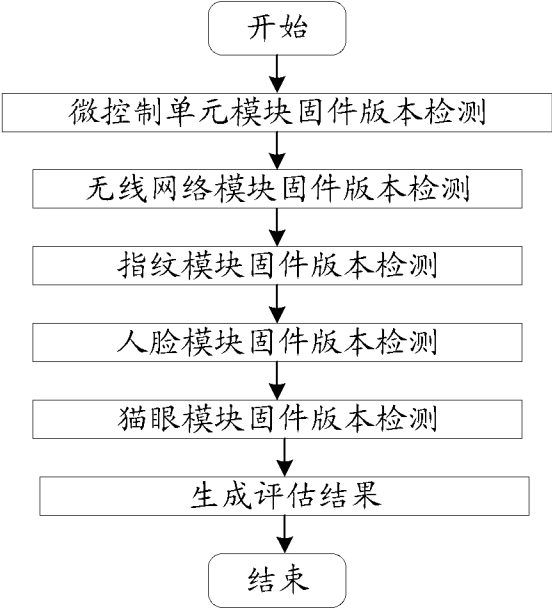


图 3b

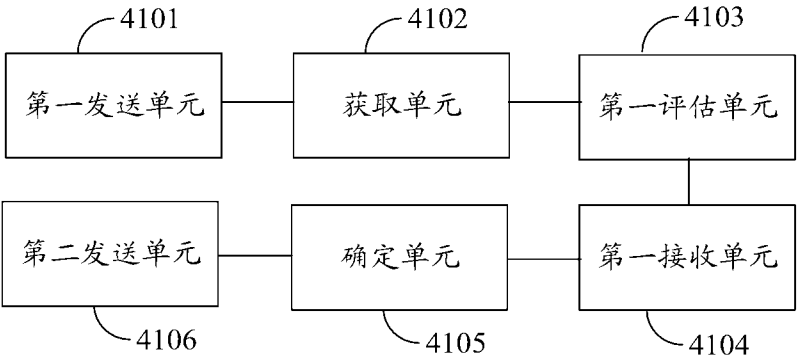


图 4a

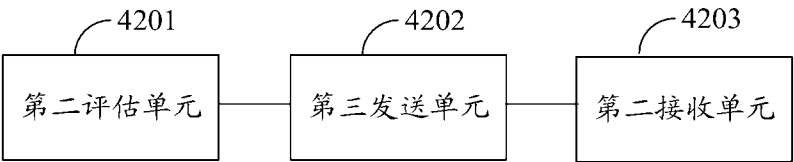


图 4b

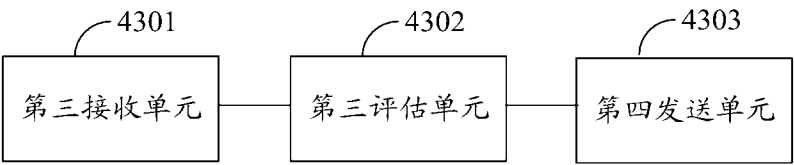


图 4c

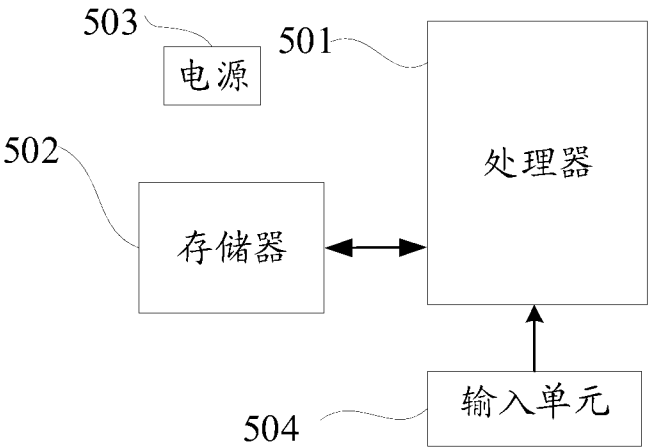


图 5

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2023/099363

A. CLASSIFICATION OF SUBJECT MATTER

H04L43/0817(2022.01)i; G07C9/00(2020.01)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)

IPC: H04L; G07C

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)

CNTXT, ENTXTC, WPABSC: 深圳TCL新技术有限公司, 罗康, 黎明德, 门锁, 云锁, 电子锁, 密码门, 密码锁, 安全, 检测, 评估, 评价, 评分, 打分, 估算, 估计, 估测, 检验, 计算, 环境, 历史, door, lock, safe+, detect, test, evaluation, examin+, calculat+, determine, environment, history

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 115311764 A (SHENZHEN TCL NEW TECHNOLOGY CO., LTD.) 08 November 2022 (2022-11-08) claims 1-15	1-15
A	CN 114758430 A (SHENZHEN LUMI UNITED TECHNOLOGY CO., LTD.) 15 July 2022 (2022-07-15) description, paragraphs [0056]-[0147], and figures 1-6	1-15
A	CN 203965141 U (CIXI XINCHANG INDUSTRIAL PRODUCT DESIGN CO., LTD.) 26 November 2014 (2014-11-26) entire document	1-15
A	CN 114399478 A (CHINA NATIONAL ENERGY RAILWAY EQUIPMENT CO., LTD. et al.) 26 April 2022 (2022-04-26) entire document	1-15
A	CN 1504626 A (MEGAWIN TECHNOLOGY CO., LTD.) 16 June 2004 (2004-06-16) entire document	1-15



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

“D” document cited by the applicant in the international application

“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

13 September 2023

Date of mailing of the international search report

21 September 2023

Name and mailing address of the ISA/CN

China National Intellectual Property Administration (ISA/
CN)
China No. 6, Xitucheng Road, Jimenqiao, Haidian District,
Beijing 100088

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2023/099363**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 113282490 A (SHENZHEN TCL NEW TECHNOLOGY CO., LTD.) 20 August 2021 (2021-08-20) entire document	1-15
A	CN 107265226 A (SHANGHAI CHENZHU INSTRUMENT CO., LTD.) 20 October 2017 (2017-10-20) entire document	1-15
A	US 2015061859 A1 (GOOGLE INC.) 05 March 2015 (2015-03-05) entire document	1-15
A	WO 2017203375 A1 (BOSCH G.M.B.H. ROBERT) 30 November 2017 (2017-11-30) entire document	1-15

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2023/099363

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	115311764	A	08 November 2022	None			
CN	114758430	A	15 July 2022	None			
CN	203965141	U	26 November 2014	None			
CN	114399478	A	26 April 2022	None			
CN	1504626	A	16 June 2004	None			
CN	113282490	A	20 August 2021	None			
CN	107265226	A	20 October 2017	None			
US	2015061859	A1	05 March 2015	US	2015112885	A1	23 April 2015
				US	10510035	B2	17 December 2019
				US	10332059	B2	25 June 2019
WO	2017203375	A1	30 November 2017	None			

国际检索报告

国际申请号

PCT/CN2023/099363

A. 主题的分类

H04L43/0817(2022.01)i; G07C9/00(2020.01)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)

IPC: H04L; G07C

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))

CNTXT, ENTXTC, WPABSC: 深圳TCL新技术有限公司, 罗康, 黎明德, 门锁, 云锁, 电子锁, 密码门, 密码锁, 安全, 检, 测, 评估, 评价, 评分, 打分, 估算, 估计, 估测, 检验, 计算, 环境, 历史, door, lock, safe+, detect, test, evaluation, examin+, calculat+, determine, environment, history

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 115311764 A (深圳TCL新技术有限公司) 2022年11月8日 (2022 - 11 - 08) 权利要求1-15	1-15
A	CN 114758430 A (深圳绿米联创科技有限公司) 2022年7月15日 (2022 - 07 - 15) 说明书第[0056]-[0147]段, 图1-6	1-15
A	CN 203965141 U (慈溪市鑫昶工业设计有限公司) 2014年11月26日 (2014 - 11 - 26) 全文	1-15
A	CN 114399478 A (国能铁路装备有限责任公司 等) 2022年4月26日 (2022 - 04 - 26) 全文	1-15
A	CN 1504626 A (笙泉科技股份有限公司) 2004年6月16日 (2004 - 06 - 16) 全文	1-15
A	CN 113282490 A (深圳TCL新技术有限公司) 2021年8月20日 (2021 - 08 - 20) 全文	1-15

☒ 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

“D” 申请人在国际申请中引证的文件

“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

2023年9月13日

国际检索报告邮寄日期

2023年9月21日

ISA/CN的名称和邮寄地址

中国国家知识产权局

中国北京市海淀区蓟门桥西土城路6号 100088

授权官员

刘晶

电话号码 (+86) 010-53962445

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
A	CN 107265226 A（上海辰竹仪表有限公司）2017年10月20日（2017 - 10 - 20） 全文	1-15
A	US 2015061859 A1（GOOGLE INC.）2015年3月5日（2015 - 03 - 05） 全文	1-15
A	WO 2017203375 A1（BOSCH G. M. B. H. ROBERT）2017年11月30日（2017 - 11 - 30） 全文	1-15

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2023/099363

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	115311764	A	2022年11月8日	无	
CN	114758430	A	2022年7月15日	无	
CN	203965141	U	2014年11月26日	无	
CN	114399478	A	2022年4月26日	无	
CN	1504626	A	2004年6月16日	无	
CN	113282490	A	2021年8月20日	无	
CN	107265226	A	2017年10月20日	无	
US	2015061859	A1	2015年3月5日	US 2015112885 A1	2015年4月23日
				US 10510035 B2	2019年12月17日
				US 10332059 B2	2019年6月25日
WO	2017203375	A1	2017年11月30日	无	