中国大学生服务外包

创新创业大赛

设备手递手——智慧设备管理系统

项目详细方案

选　　题：【A14】移动互联时代的设备管理【虹软】

团队编号：2003416

目 录

1 背景、痛点与系统功能

1.1 背景介绍

随着设备或信息价值的不断提升，各企业对设备资产，尤其是重要设备及保密设备的重视程度愈来愈高。如果相关设备发生丢失或泄密，将会给自身及合作企业带来重大损失。因此，一套兼具安全性与便利性的设备管理方案成为各企业的刚性需求。

1.2 痛点分析

现阶段各企业设备管理主要存在以下痛点：

- 设备登记、注销不便，公司设备盘点费时费力。
- 设备转借、私下流通登记不便，设备丢失难以追踪、追责。
- 设备非正常带出公司难以检测，泄密隐患尤为棘手。

1.3 系统功能

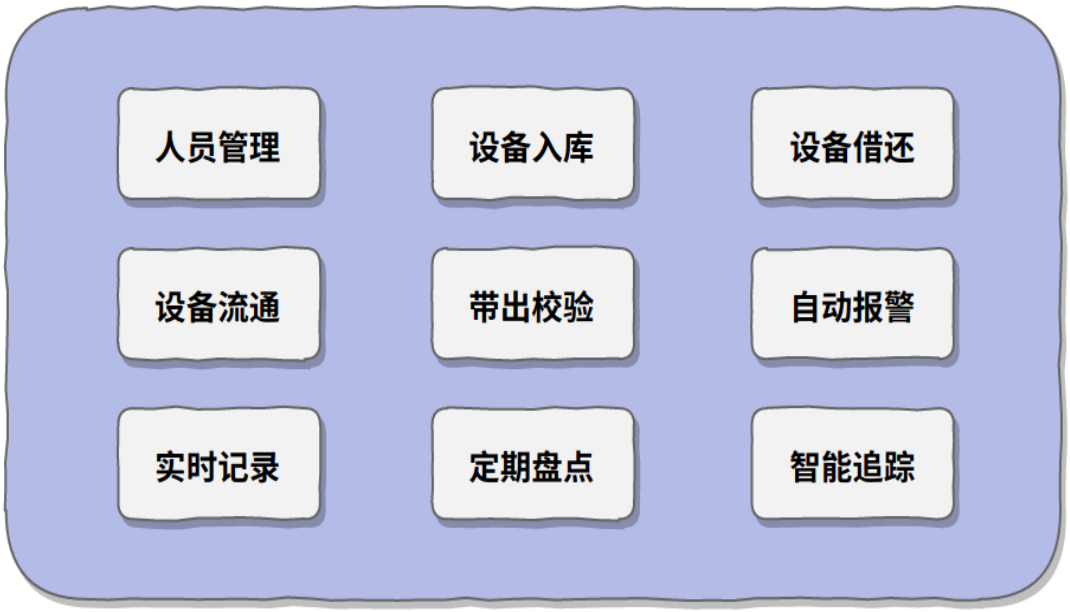


图 1 系统功能图

1. 设备登记注销

入库新设备可生成 Excel 表格导入系统实现**批量登记**，不再管理的设备可一键注销。

2. 设备分级管理

系统将设备分为常规设备、重要设备、保密设备三个等级，针对不同等级的设备系统采取不同的借还方案及带出限制。

- **设备便捷流通及实时记录**

员工可通过微信小程序扫描设备二维码或 NFC 功能借用设备，每次设备借用人变更都会生成相关变更记录。方便管理实时跟进设备状态及问题追责。

- **设备非正常带出自动报警与记录**

通过在公司出口门禁处安装 RFID 扫描装置及人脸识别系统，校验设备携带者相关携带行为是否合法，采取相应的放行策略及报警机制，实时拍摄并记录非法人员的人像信息。

3. **设备定期盘点**

在系统中，管理人员可便捷查看在库设备清单、出借设备清单及借用人员信息。

2 系统总体设计

2.1 系统架构

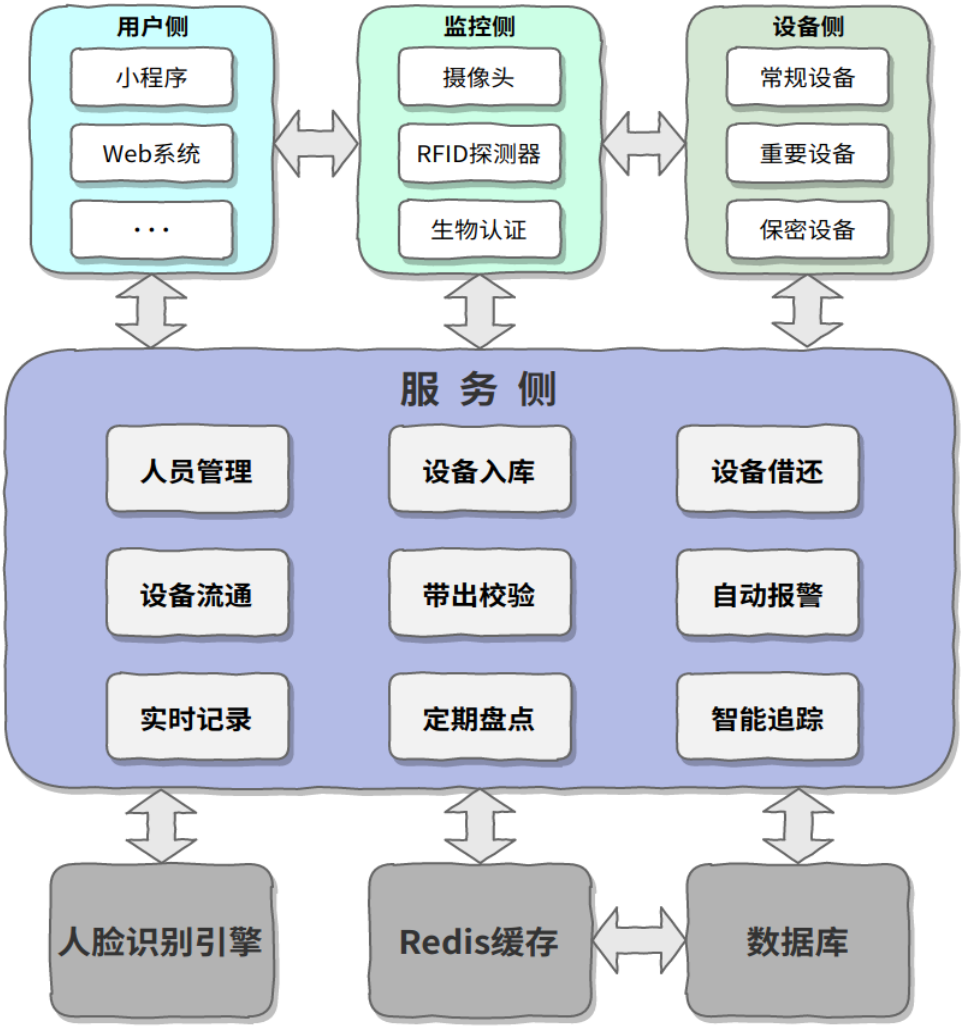


图 2 系统架构图

如上图所示，该系统主要分为用户侧、监控侧、设备侧、服务侧，不同的模块协同完成对设备的相关管理工作。

1. **用户侧**

该系统中，用户分为普通员工和系统管理员。普通员工主要通过**微信小程序**使用该系统，完成设备借还、转借等动作，系统管理员则主要在 **Web 管理系统**中对设备出借、归还、盘点及追踪进行统一管理。

2. 监控侧

该系统中，对设备以及设备借用人员的实时监控主要通过智能摄像头、RFID 探测器以及智能手机的生物认证功能实现。

◆ **智能摄像头**

当员工存在设备带出行为时，相关的智能摄像头会拍摄设备带出者的实时图片用于后续的校验机制。

◆ **RFID 探测器**

在公司出口道闸处安装有此设备，当有相关设备经过道闸时，探测器会自动**捕获设备相关信息**，结合摄像头拍摄的人像信息，系统自动校验设备带出的合法性。

◆ **生物认证**

这里主要指的是智能手机的**面容 ID** 及**指纹识别**功能，借此防范员工使用他人手机进行借还设备等作弊行为。

3. **设备侧**

根据对企业需求的分析结果，企业需要管理的设备主要可以分为以下三类。**常规设备，重要设备，保密设备**。在该系统的设计中，针对三种不同等级的设备，带出时系统会采取不同的放行策略，借出时的限制条件也会有所差异。

◆ **常规设备**

系统对常规设备的借还权限没有限制，当该类设备被带出时，只要通过人脸识别认证，即确保携带人与借用人为同一人，方可放行。同时系统会自动生成一条该设备的带出记录。

◆ **重要设备**

系统对重要设备的借还没有限制，但对该类设备的**带出做出了限制**。一旦该类设备被检测到带出行为。系统会自动触发报警机制，保护该设备不被带出公司。

◆ **保密设备**

系统对保密设备不仅做出了**带出限制**，还对其做出了**借还限制**。该类设备严禁带出公司，一旦检测到带出行为，系统会自动报警。该类设备的借还工作必须由仓储管理人员完成，并且不允许该类设备在公司内部私自流通、转借。

4. **服务侧**

该系统依托于人脸识别引擎及相关基础设施实现了对人员、设备的安全高效管理。

◆ **功能性**

该系统的功能主要为两个大的方面，一方面是**对于人事信息的灵活管理**，主要包括导入公司人事表为员工自动创建账号，公司人员信息异动实时更新；另一方面是**对于设备的高效管理**，包括设备入库，设备借还，设备流通，带出检测，自动报警，实时记录，定期盘点，智能追踪等。

◆ **人脸识别引擎**

在检测到设备带出时，通过人脸识别引擎对携带者进行人脸校验，判定本次携带行为是否合法。

◆ **数据持久存储**

员工基本信息、人像特征信息、设备信息、借还记录以及报警记录等数据都会在数据库持久存储，为相关功能提供数据支持，比如设备定期盘点及设备追踪。

2.2 场景示意

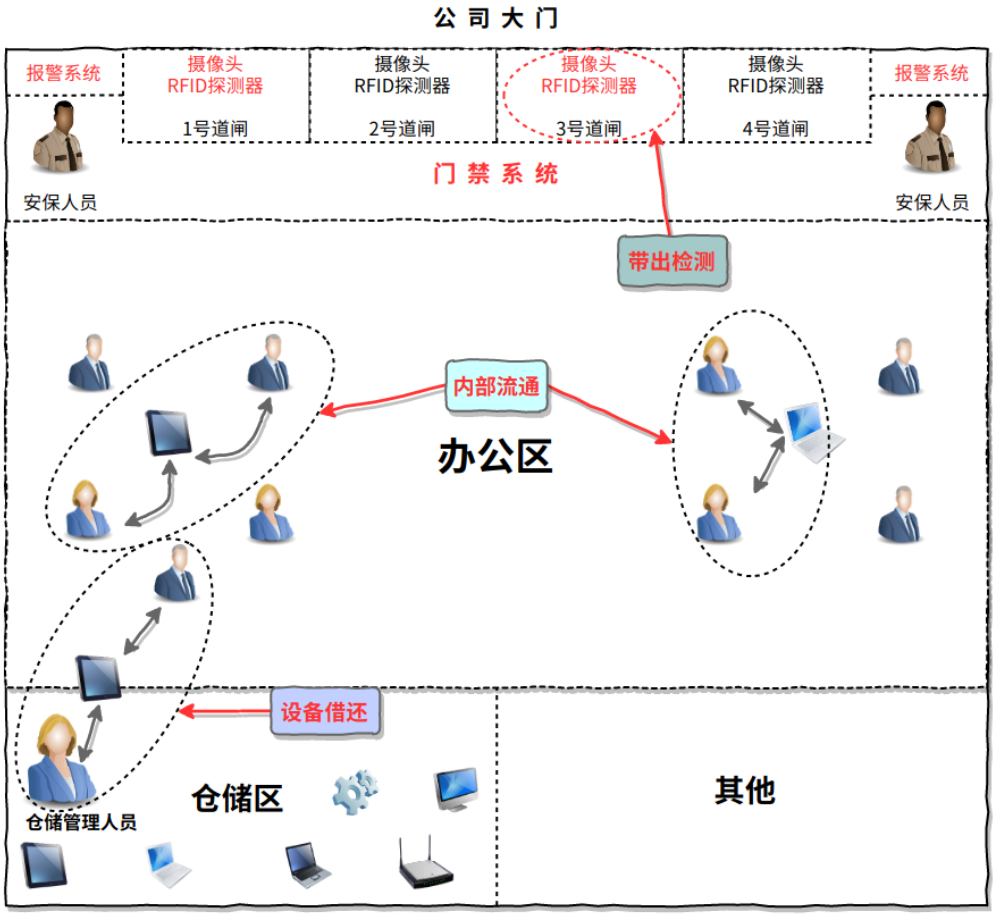


图 3 公司平面示意图

如上图公司平面示意图所示，将公司相关活动区域简单划分为以下四类，**仓储区**，用于存放系统管理的设备；**办公区**，员工活动区域；**公司大门**，即门禁系统安装区域，以及**其他区域**。发生在公司的关于设备的活动主要为三类：在仓储区发生的**设备借还**动作，在办公区发生的**内部流通**动作，在公司出口处的设备**带出检测**。

- ✧ **设备借还：**即员工在仓储区向仓储管理人员借用设备或归还设备。
- ✧ **内部流通：**即**员工之间进行的设备转借行为，不经过仓储管理人员**。但该种行为只支持常规设备，在详细设计中会进行相关详尽阐述。
- ✧ **带出检测：**即在企业出口处，会安装相关设施对经过的人员、设备进行相关检测，校验行为合法性。

3 系统详细设计

3.1 设备侧

3.1.1 RFID 标签、二维码绑定设备 ID

在该系统设计中，需要在被管理的每一个设备上固定一个 RFID 标签，**该 RFID 标签上同时印刷着绑定了设备 ID 的二维码**，在设备借还以及设备内部流通的过程中，将会基于扫描二维码或者 RFID 实现。在设备带出检测环节中，会基于上文提到的超高频 RFID 探测器探测设备上的 RFID 标签信号。在后续的校验报警流程中将会着重阐述设备带出合法性的校验机制。

超高频 RFID 标签采用 ISO18000-6C 生产标准，工作频率为 860MHz-960Mhz，识别距离约 6m（与实际采集设备功率有关），标签内部数据可反复读取 100000 次，数据保存 10 年以上。

图 4 RFID 标签

在该系统设计中主要采用如上图所示的 Imping M4E 芯片正方形标签，拥有高达 496bits 可编程 EPC（Electronic Product Code）设备编号，128bit 可自定义 User 区，能够写入自定义数据。标签另一侧可印刷二维码。

图 5 标签粘贴示意图

读距约：12米（视读写器读距而定）　　整卷数量：300张

名　　称：	柔性抗金属标签	品　　牌：	WYUAN
产品型号：	PF10040	尺寸规格：	100*40mm
工作频率：	860MHz～960MHz	工作协议：	ISO18000-6C
材　　质：	铁氟龙+PET	芯片类型：	IMPINJ MR6-P
工作温度：	-20℃~75℃	存储容量：	EPC128bits

图 6 柔性抗金属标签

名　　称：	PCB抗金属耐高温标签	品　　牌：	WYUAN
工作温度：	-40℃～+150℃	尺寸规格：	多种尺寸可选
工作频率：	860-960MHz	芯片类型：	ALIEN H3
符合标准：	ISO18000-6C	存储容量：	EPC 96bits
材　　质：	PCB	产品特性：	抗金属、耐高温
使用期限：	可读写100000次，数据保存10年		

图 7 抗金属抗高温标签

此外针对不同的设备，也可以采用上图所示的抗金属柔性 RFID 标签、抗金属耐高温 RFID 标签，满足多场景设备管理需要。

防作弊策略：考虑到存在人为撕毁相关柔性标签的可能性，可以将上图所展示的标签嵌于设备内部，二维码单独粘贴于设备合适位置，提供便捷的同时兼顾安全性。

3.1.2 设备分类、分级管理

根据对相关企业的需求分析结果，企业中需要管理的设备大致可以分为以下三类或三种等级。等级从低至高依次为：**常规设备**，**重要设备**，**保密设备**。针对三种不同

等级的设备，系统在检测到相关设备被带出时会采取不同的放行策略，不同设备在进行借出时的相关限制条件也有所差异。力求对设备做到全面、合理的管理。

3.1.3 各类设备借还、带出策略定制化

表 1 各类设备借还、带出定制化策略

	常规设备	重要设备	保密设备
借用限制	×	×	√
可私下流通	√	√	×
可带出公司	√	×	×

- **常规设备**

主要指企业中的工具类设备，**比如一些鼠标、键盘**。系统对常规设备的借还没有限制；当该类设备被带出时，只要人脸核验通过，方可放行。当然，系统也会实时生成该设备的带出记录。该带出记录主要包含以下几点关键信息：设备 ID、携带人 ID、携带时间。该记录可用于后期的设备盘点及实时追踪。

- **重要设备**

主要指具有一定保密性质，但保密程度不高的仅用于开发设备，**比如某合作企业提供的工程样机**。系统对重要设备的借还行为采取和常规设备同样的策略，但对该类设备的带出采取了相关的拒绝策略。一旦该类设备被检测到被带出。系统会自动触发报警机制，即开启警报系统，提示安保人员对相关设备进行核验。同时，系统也会生成该设备的报警记录。该报警记录主要包含以下几点信息：设备 ID、携带人照片、报警时间、报警级别。

- **保密设备**

主要指公司研发的、需要保护其知识产权的等绝密设备，**比如企业研发的带有特定功能的未加密的摄像头样机**。系统对保密设备不仅采取了带出拒绝策略，还对该类设备做出了借还限制。与重要设备相同，一旦检测到设备被带出，便会触发报警机制，提示安保人员进行核验，同时也会生成与重要设备类似的报警记录，不同之处在于，这里的报警级别更高。在针对该类设备的借还机制中，系统也做出了相关限制，即**保密设备的借还工作必须由仓储管理人员完成，不允许该类设备在公司内部私自流通、转借**。若该类设备出现相关安全问题，可直接追究借用人的责任。

3.2 监控侧

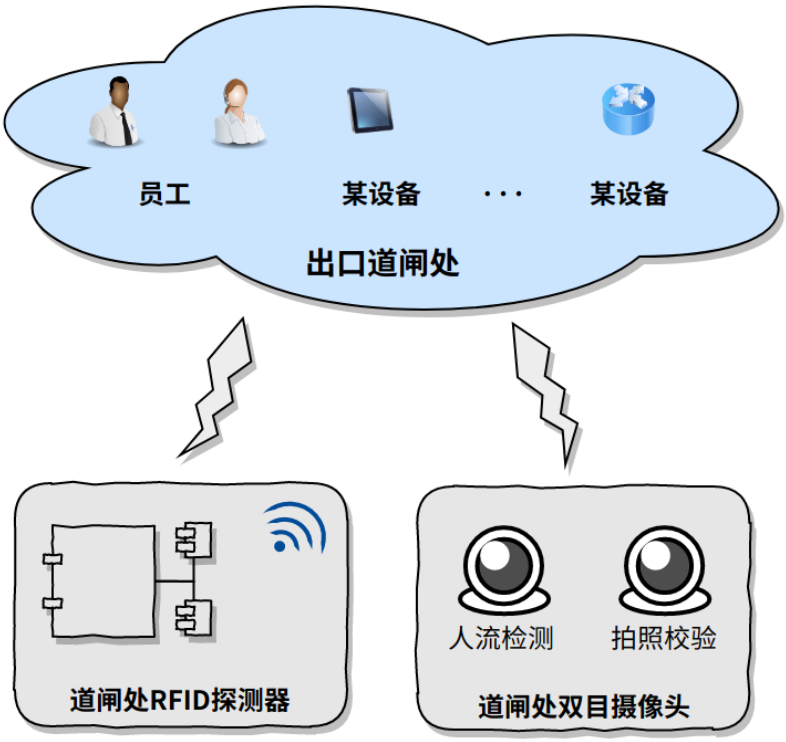


图 8 布控示意图

3.2.1 超高频 RFID 探测器实时监控设备

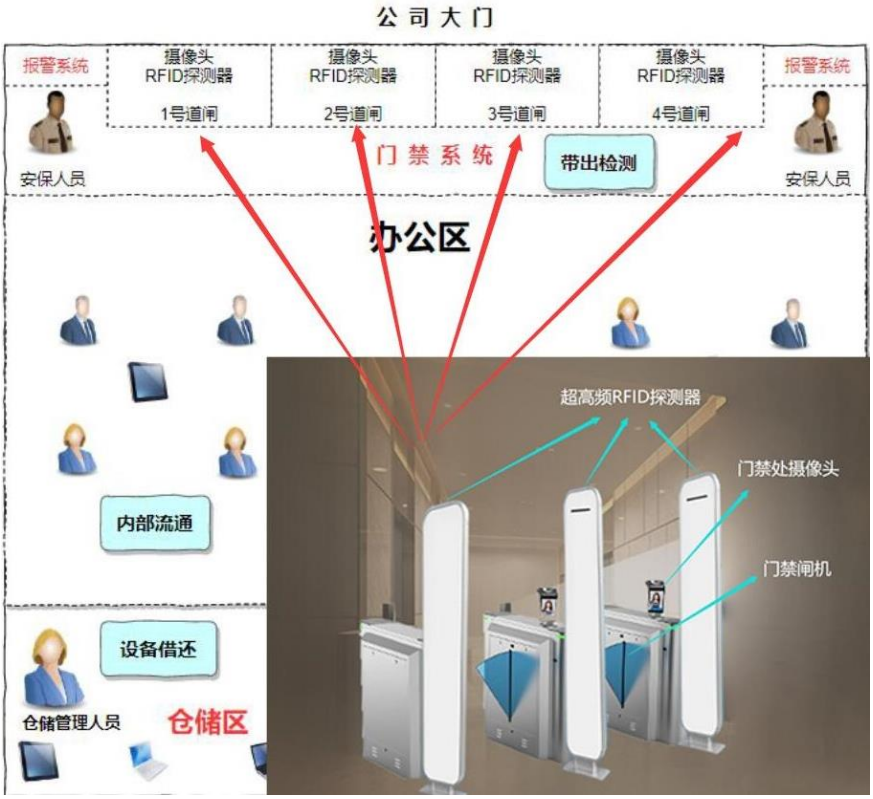


图 9 RFID 探测设备安装示意图

如上图所示，该系统假设公司有统一的入口道闸和出口道闸，这里的相关设备安装的位置为公司的出口道闸处，每一个道闸口都安装有上图所示的 RFID 探测器及摄像头。实现对出入设备的全方位检测，避免相关设备被带出公司造成不必要的损失。

图 10 超高频 RFID 探测器

RFID 为射频识别技术，其原理为阅读器与标签之间进行非接触式的数据通信，达到识别目标的目的。该系统使用超高频 RFID 技术，即 UFD，射频频率在 850MHz-950MHz 之间，一般使用 920MHz 左右的频率波段进行探测，确保频段唯一。该系统在设备录入的时候给每一个设备分配一个唯一 RFID 标签，标签内部包含可编程的 ID 序列号。将 ID 序列号设置为唯一后，带有此标签的设备进出道闸时会被 RFID 探测器所扫描识别，获取 ID 号。RFID 探测器的探测范围与探测器设置和探测天线的增益、天线朝向等有关，可以调整为道闸中心距离 1m 内进行辐射式扫描读取。同时，RFID 探测器实现了支持防冲撞的群读算法，读取速度最大 200 枚标签每秒，一般设置为每秒扫描 10 至 50 次。

此外，可供选择的 RFID 标签也有多种，有防撕毁标签、抗金属标签、耐高温标签、柔性标签、防水标签等，可根据具体设备实际需要进行标签选择。

3.2.2 智能摄像头实时监控带出行为

图 11 摄像头安装示意

该系统设计中，前文已经提到需要在相关地方安装摄像头，这里具体深入地阐述摄像头的安放细节。首先，此处摄像头与道口闸机为一体机，方便准确拍摄清晰、有效的人脸照片。其次，该类摄像头需为**双目摄像头，一枚用于人流实时监测，另一枚专门用于拍照。**

站在用电量和系统负荷的角度考虑，在该系统设计中，道闸处的相关监测设施**并不会一直处于高功率运行状态**。如下图所示，当人流检测摄像头**检测到人流时**，将会**触发 RFID 探测器的探测机制**，扫描该行人是否有携带相关设备进出公司。若探测到有相关设备被带出，另一枚摄像头随即拍摄相关照片进行校验是否合法。实现对设备、人员的实时监控。

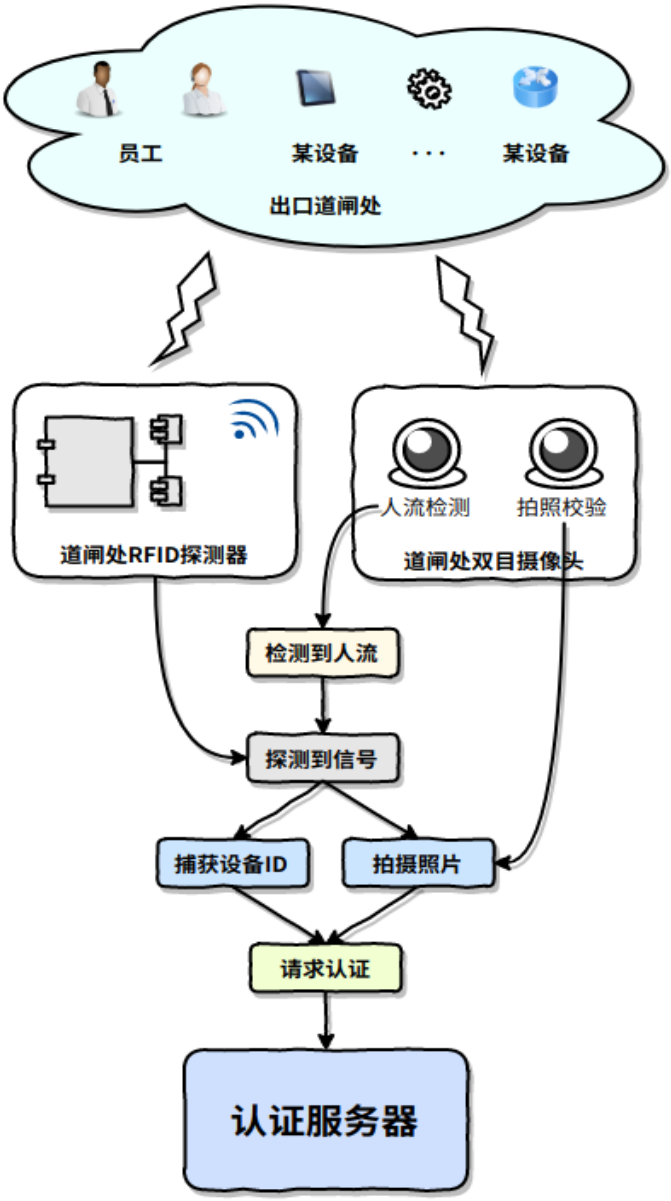


图 12 门禁系统运行机制

3.2.3 生物认证机制确保操作真实合法性

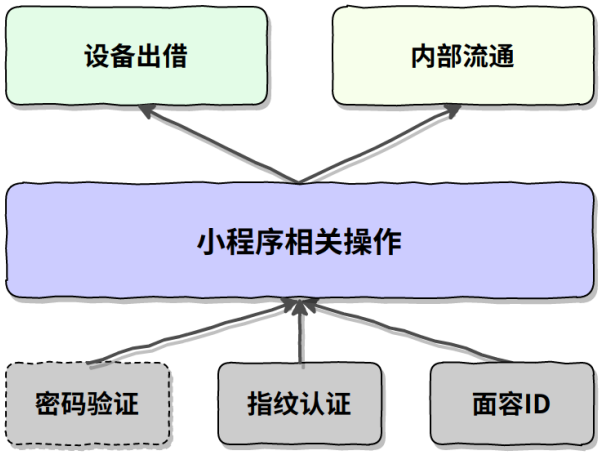


图 13 小程序相关操作示意图

该系统中，采用生物认证机制来确保员工在小程序中相关操作的真实性与合法性。员工使用小程序扫描待借设备上的二维码后，需进行身份认证，身份认证可以通过指纹、面容 ID 或密码三种方式完成。

- ✧ 对于具有**指纹识别**功能的手机，员工可以使用指纹功能，便捷实现身份认证。
- ✧ 对于不具备指纹识别，但具有**面容 ID** 的手机，用户可以使用核验面容 ID 的方式，同样可以完成身份认证。
- ✧ 对于不支持以上两种生物认证的手机，用户可以**输入密码**进行身份认证，兼顾各种使用情况。

生物认证机制可以有效**防止人为作弊**情况的发生，确保了对设备进行操作的人与小程序端登录账号的一致性，保障操作真实性以及合法性。

3.3 服务侧

3.3.1 系统功能设计

1. 人事管理

- 录入员工信息

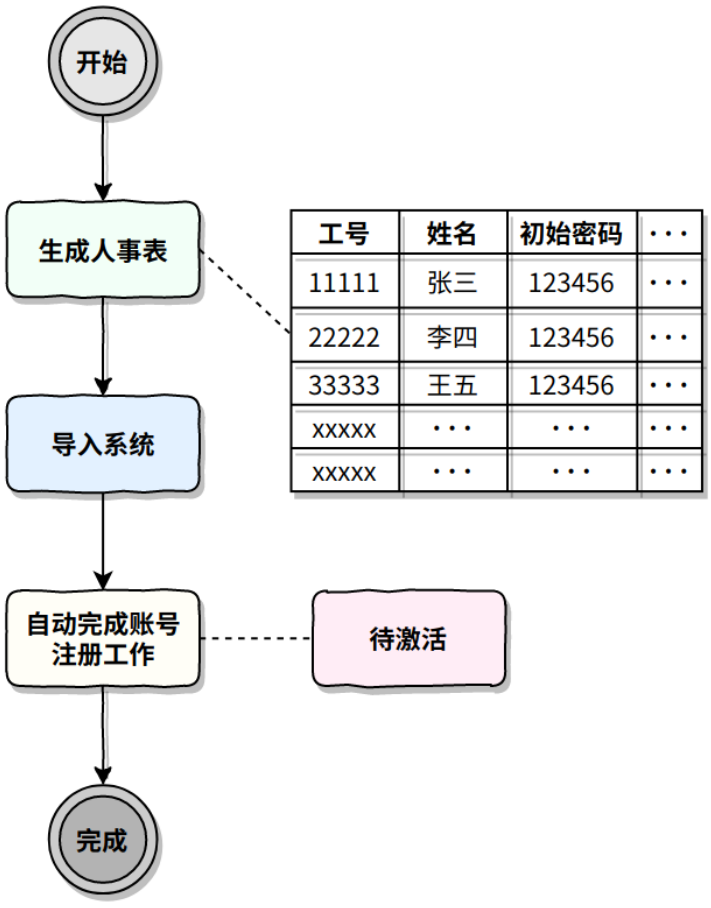


图 14 人事信息录入流程

如上图所示，为了降低企业的使用成本，在录入人事信息时，支持并推荐通过生成 excel 人事表（主要包含员工工号、姓名、登录初始密码等），导入系统实现**批量导入员工信息**，系统会自动为各员工创建账号，当员工使用小程序进行**首次登录**时，需要上传一张证件照用来激活账号，具体激活流程见下文激活流程。

当然，若企业内部存在相关的人员变动，管理人员也能针对单个员工信息进行相关管理。

- 账号激活

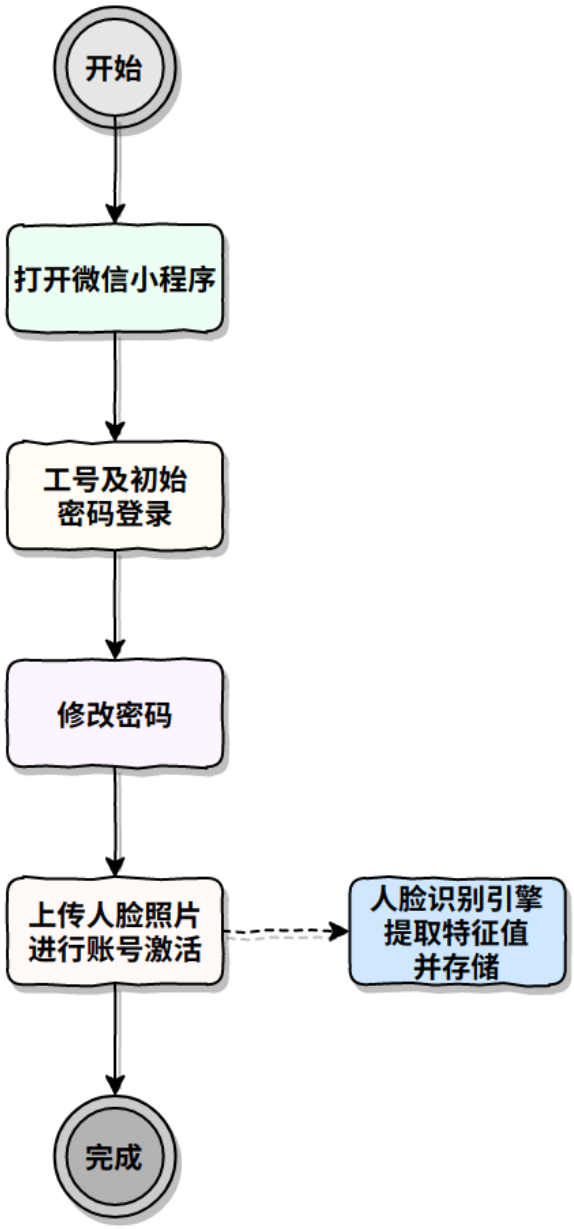


图 15 员工使用激活流程

员工在使用系统前，需要进行账户激活操作。

✧ 如上图所示，员工进入微信小程序界面，输入工号以及初始登录密码完成登录操作。

✧ 随后系统会要求员工进行修改密码。

✧ 修改成功后会进一步要求员工上传本人照片进行特征值提取，人脸识别引擎将对上传的照片进行人脸目标检测，并将照片特征值存储于后台。这一步完成标志着账号激活成功。

✧ 随后会自动重新登录，方可继续使用相关功能。

2. 设备入库

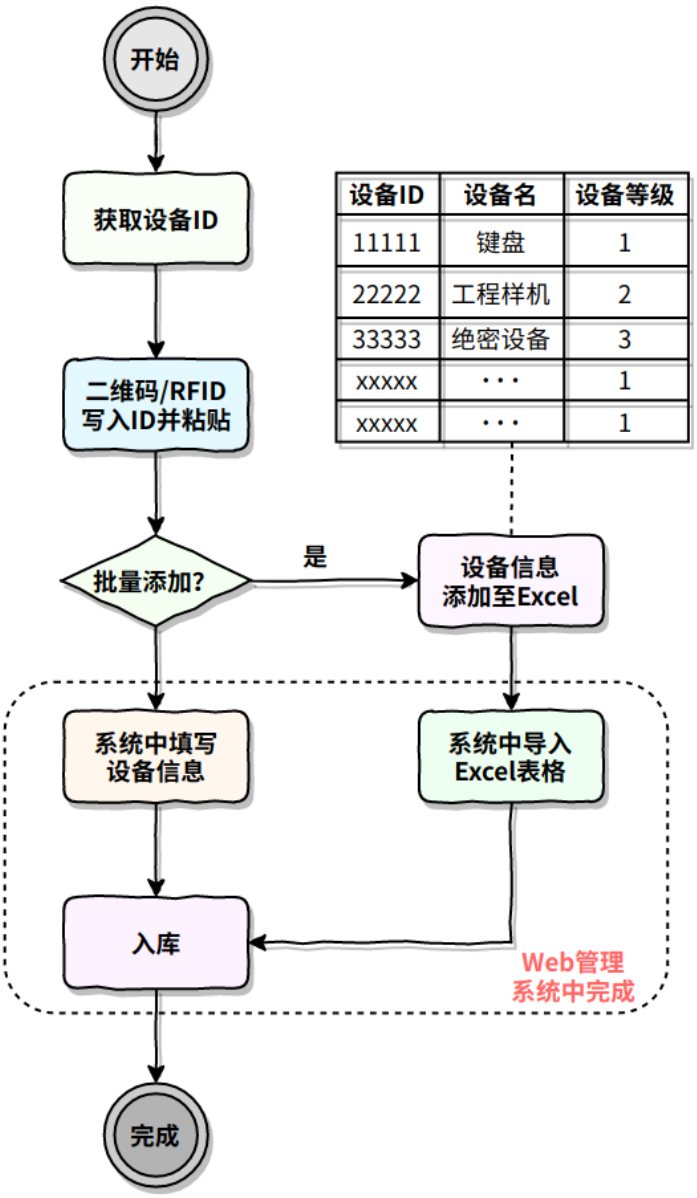


图 16 设备入库流程

当企业入库一批新设备时，需要将这些新设备添加到系统，方便管理人员对其进行统一的管理。

入库流程如上图所示：

✧ 设备入库前需要为该设备生成一个设备 ID，这个 ID 可以来源于生产厂商，也可以是系统为其设计的。

✧ 将该设备 ID 写入到一张 RFID 芯片，同时这张 RFID 芯片背后的二维码存储的信息

也会是该设备的 ID。

✧ 将该芯片粘贴到设备的合适位置。

✧ 执行添加设备操作，如果管理员需要批量添加设备，仅需要将该设备的相关信息添加到 Excel 表格即可，表格的字段主要包含以下信息：设备 ID、设备名、设备等级。

✧ 将 Excel 表格导入系统或者将某个设备直接添加到系统后，即完成了设备的入库流程。

3. 设备借还

- 设备出借

该系统同时提供了两种流程供借用人员根据实际情况进行选用。

✧ 第一种为半自助方式，即借用人员通过微信小程序自主完成相关流程，只需要在正式交付设备之前向管理人员出示相关信息即可。

✧ 第二种方式为管理人员完成设备借出的一系列动作。这种方式主要适用于当员工来到设备管理处发现没有携带手机，或者手机出现相关故障无法顺利使用小程序的场景。

下面详细阐述两种设备借用方式的流程。

◆ 半自助方式

如下图（左）所示，借用人员提出设备借出请求后，仓储管理人员取出设备，获得对应设备的二维码或 RFID，借用人员利用小程序获取设备信息，录入方式可采用前文所述的二维码扫描或者 RFID 扫描两种方式，在成功获取设备信息之后，发起借用请求之前，需要进行生物认证，即验证本次借用行为的合法性。认证途径包括指纹识别、面容 ID，如果以上两种方式均出现故障或不方便使用，还可以通过输入账号密码进行认证。借用人员在生物认证通过后，借用请求成功发出，若该设备为绝密设备，则拒绝本次借用，需要由管理员进行完成借出动作。若非绝密设备，当系统返回借用结果后，需要向仓储管理人员出示借用结果，以确保设备出借的安全性，防止人员借出作弊，仓储人员确认借用结果后，方可将设备交付于借用人员。上述流程即为通过半自助的方式完成一次设备借用流程。

◆ 仓储人员完成借出动作

如下图（右）所示，借用人员提出设备借出请求后，仓储管理人员取出相关设备便开始执行相关的借出登记工作。首先管理人员需要在管理系统中录入借用人员相关信息，可以采用工牌扫描或者手动录入的方式。然后进行设备录入操作，可以采用二维码扫描、RFID 扫描或者手工录入的方式，上述的操作结束后即可交付设备。

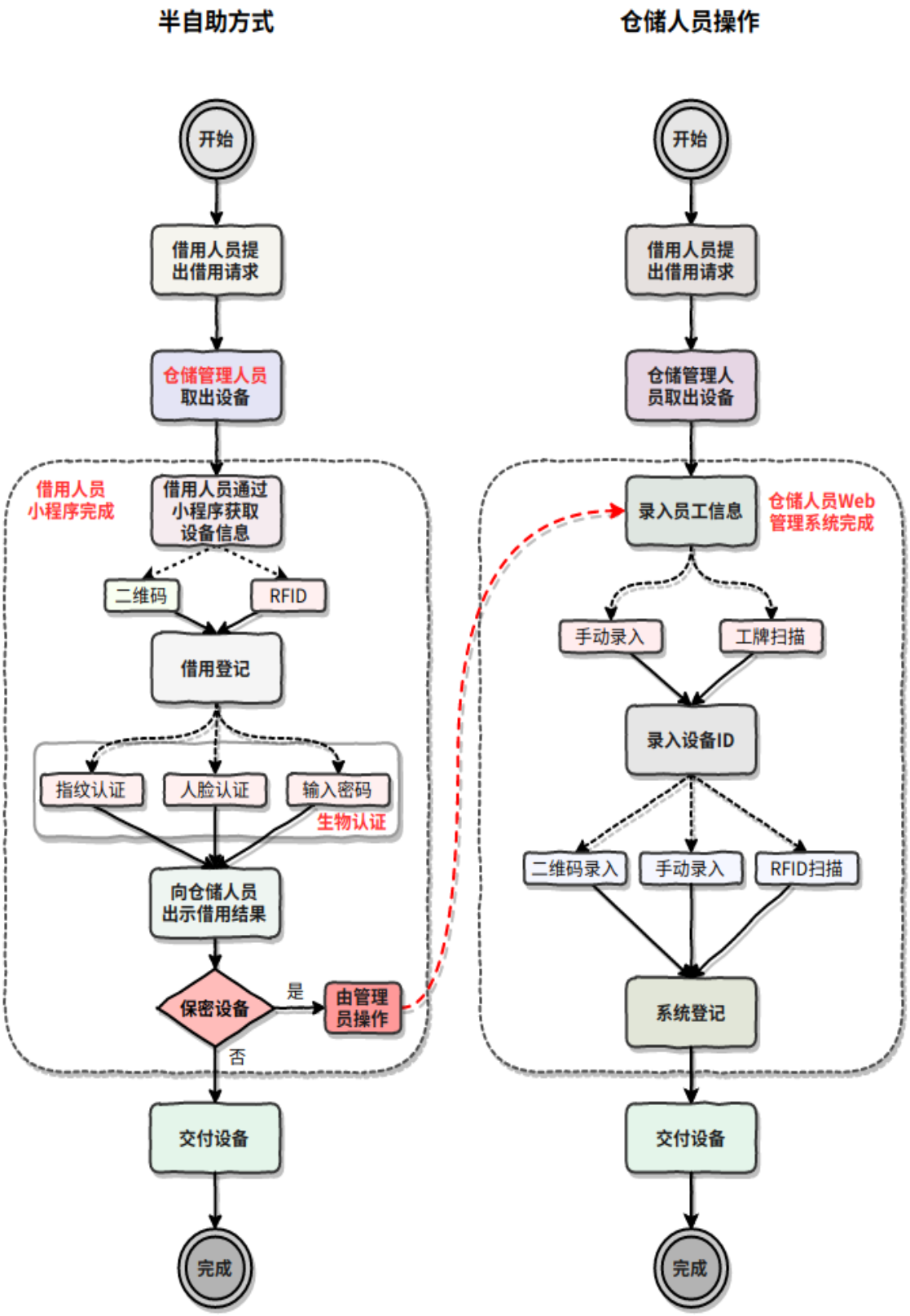

半自助方式
仓储人员操作
开始
借用人员提出借用请求
仓储管理人员取出设备
借用人员小程序完成
借用人员通过小程序获取设备信息
二维码
RFID
借用登记
指纹认证
人脸认证
输入密码
生物认证
向仓储人员出示借用结果
保密设备
是
由管理员操作
否
交付设备
完成
开始
借用人员提出借用请求
仓储管理人员取出设备
录入员工信息
仓储人员Web管理系统完成
手动录入
工牌扫描
录入设备ID
二维码录入
手动录入
RFID扫描
系统登记
交付设备
完成

图 17 设备出借流程

- 设备归还

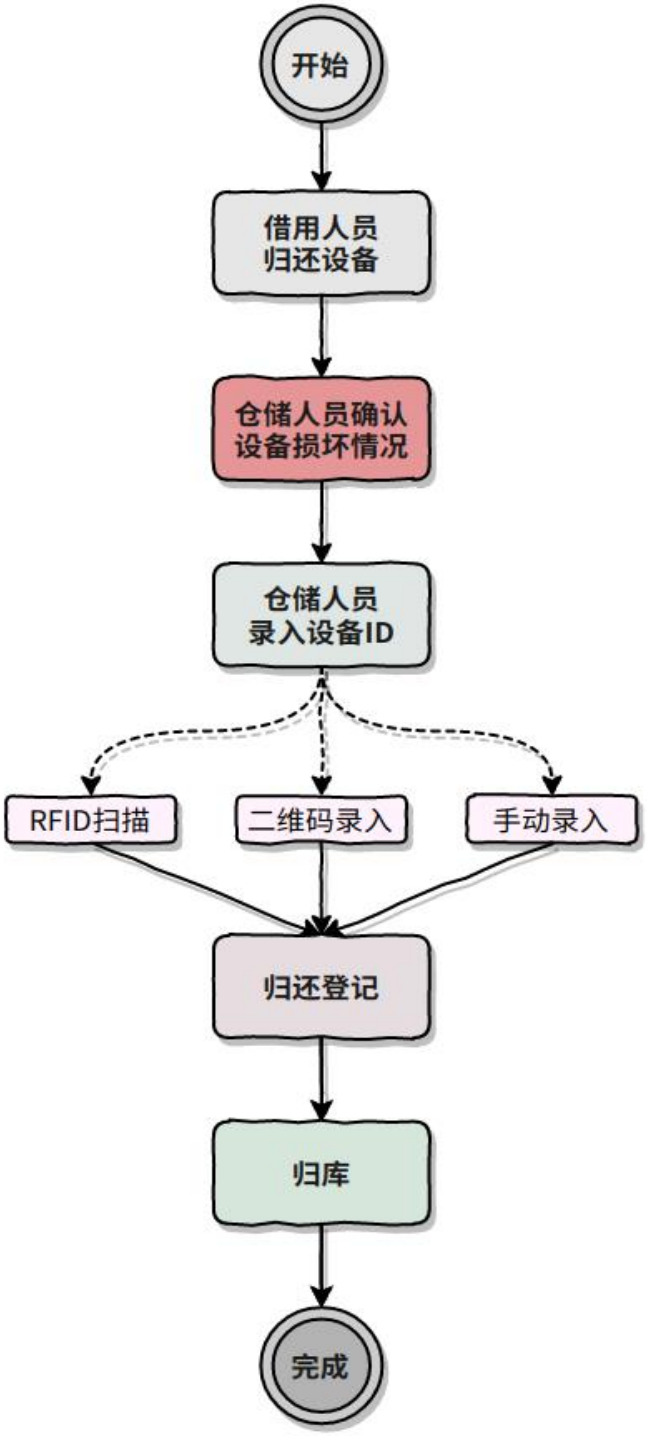


图 18 设备归还流程

✧ 借用人员需要归还设备时，仓储管理人员首先会审核设备是否存在损坏情况。

✧ 确认设备无损后，管理人员才会继续执行后续的设备归库流程，主要为获取设备 ID，这里可采用二维码扫描、RFID 扫描或者手动录入设备 ID 的方式。

✧ 录入成功后，在管理系统更新设备的状态，将设备置于仓库中合适位置即完成了设备归还流程。

4. 设备内部流通

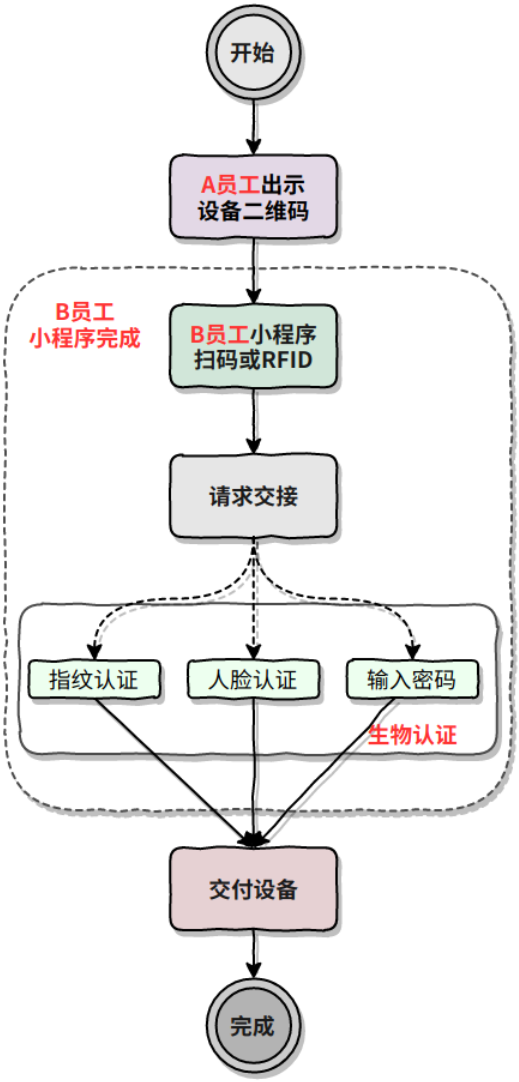


图 19 设备私下流通流程

在该系统设计中，允许非保密设备在员工之间私下流通，当然，私下流通也需要员工通过小程序进行相关登记。若私下流通不进行登记，该系统认为这种行为是非法的不可控的行为，若设备出现相关问题，将追究系统中所记录当前持有者的责任。

设备私下流通的具体流程如上图所示：

- ✧ A 员工（第一借用人）向 B 员工（第二借用人）出示设备二维码或者 RFID。
- ✧ B 员工通过微信小程序扫描二维码或 RFID，向 A 员工发起借用请求，这里发起借用请求同样需要相关进行相关认证，避免作弊行为。
- ✧ 认证通过后 A 员工交付设备于 B，即完成了一次设备内部流通。

5. 设备带出校验

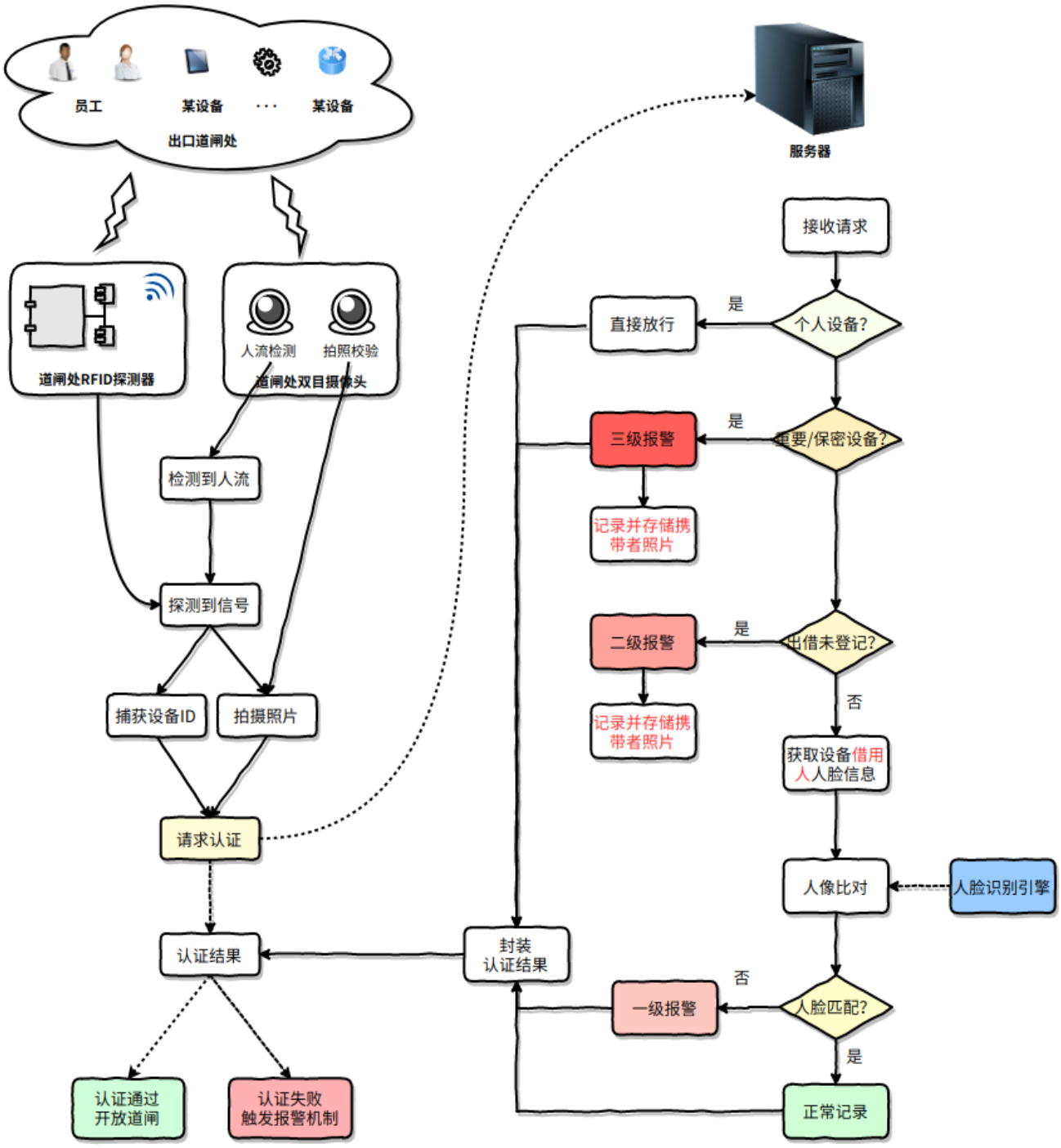


图 20 检测、报警及记录流程

根据企业的相关需求以及上分做出的分析假设，针对不同等级的设备带出行为，系统会采取不同的放行策略。所以，为了对常规设备、重要设备及保密设备进行合理、规范、安全的管理，该系统设计了严格的带出校验机制。

具体流程如上图所示：

✧ 基于前文关于监控侧的设计，即在企业出口的每个道闸处安装相关的闸机、超高频 RFID 探测器以及双目摄像头。

- ✧ 当道闸监控系统启动后，人流检测摄像头将一直处于工作状态，用于检测人流经过情况。
- ✧ 当人流检测摄像头检测到人流经过，将会激活 RFID 探测器的工作状态，RFID 探测器开始探测行人是否有将相关设备带出企业。
- ✧ 若检测到相关信号，系统会捕获设备 ID，与此同时触发专门用于拍照的摄像头对行人拍照，向服务器发起认证请求，请求本次带出行为是否合法。
- ✧ 当服务器收到门禁系统的认证请求后，会判断设备是否为个人设备，即设备并未在系统管辖范围之内。若为个人设备则认证通过，向门禁系统返回认证结果。若为系统管理设备则会继续执行后续的校验机制。
- ✧ 若系统探测到的设备为重要设备或保密设备，系统判定为认证失败，返回认证结果的同时生成一条三级报警记录，携带者照片在服务器进行存储。
- ✧ 若设备为常规设备，系统首先会查询该设备借用人 ID，如果设备 holder_id（即借用人 ID）为 NULL，即该设备正常情况下应该在库中，系统同样判定为认证失败，返回认证结果的同时会生成一条二级报警记录，携带者照片在服务器进行存储。
- ✧ 若借用人 ID 不为空，则会进行人脸校验，即根据借用人 ID 查询该借用人人脸特征信息，再通过人脸识别引擎提取门禁系统中摄像头所拍摄的携带人图片特征值，通过人脸识别引擎对二者进行比对，确认借用者、携带者是否为同一人。
- ✧ 若借用者、携带者被判定为同一人，则认证通过，返回认证结果同时生成该设备的正常带出记录，这里不存储携带者照片。
- ✧ 若二者被判定为非同一人，则认证失败，返回认证结果的同时会生成该设备的一级报警记录，并存储携带者照片。
- ✧ 相关认证结果返回后，门禁系统根据返回的认证结果触发相关的报警机制，只有认证通过才会打开道闸，认证失败会触发报警机制，提醒门禁处安保人员进行相关核验，人工处置，人工放行。

若检测到同时**带出多台设备**，在请求校验时，请求数据中将包含该人员携带的设备 ID 列表。系统会**对每台设备都进行相关校验，只要这些设备中存在设备被非法带出，都会认证失败，并且所有设备的相关携带行为都会被系统记录。**

6. 自动报警

在上一节关于设备带出校验的分析中提到，当设备带出并被检测到，门禁系统会请求认证携带的合法性，门禁系统根据认证结果会自动触发相关报警机制。

7. 实时记录

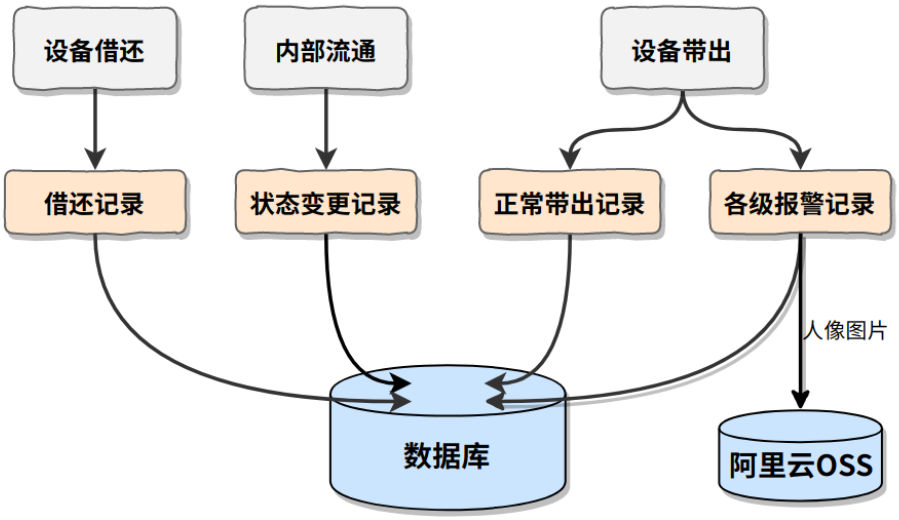
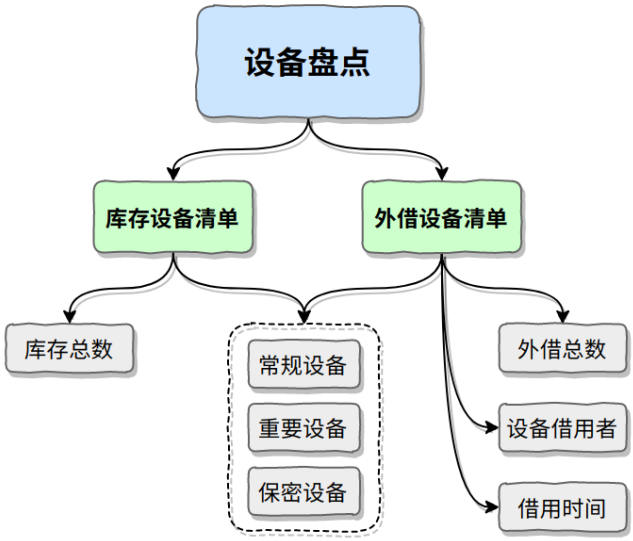


图 21 实时记录

如上图所示，该系统在对设备管理的相关环节中，都会进行实时记录。主要包括设备借出、设备归还时产生的相关借还记录，设备在进行私下流通时产生的设备状态变更记录，以及设备带出时产生的正常带出记录及各等级的报警记录。

8. 定期盘点



常规设备库存清单

设备ID	设备名	归库时间
111	设备1	2020.2.20
222	设备2	2020.2.21
333	设备3	2020.2.22
444	设备4	2020.2.20
···	···	···

重要设备外借清单

设备ID	设备名	借用人	借用时间
111	设备1	张三	2020.2.20
222	设备2	李四	2020.2.21
333	设备3	王五	2020.2.22
444	设备4	赵六	2020.2.20
···	···	···	···

图 22 设备盘点

如上图所示，当管理人员通过该系统定期对设备进行盘点时，系统会分别给出库存设备清单、外借设备清单。

- ✧ 库存设备清单，主要包括库存设备总数，常规、重要、保密各级设备的清单，方便管理人员及时掌握设备的库存情况。
- ✧ 外借设备清单，同样包括设备外借设备总数，以及各类设备清单，同时清单还给出了各设备的借用者信息及借用时间。方便设备管理员对外借设备进行实时跟进，确保设备安全状态。

9. 实时追踪

在该系统设计中，可以实现对相关设备的实时追踪，即实时掌握当前设备状态，主要为被谁持有，并导出某个设备的相关借还记录，相关带出记录及相关报警记录，根据相关记录可溯源该设备相关状态，实时跟进设备的动态，动态掌握设备行踪。

表 2 设备追踪表

行为	执行时间	执行人信息
借出	2021.3.28 10:23:43	员工 A
归还	2021.3.28 19:34:31	员工 A
借出	2021.3.29 10:23:43	员工 B
私下流通	2021.3.29 11:26:53	员工 C
带出	2021.3.29 20:23:43	员工 C
私下流通	2021.3.30 10:12:03	员工 D

3.3.2 人脸识别引擎

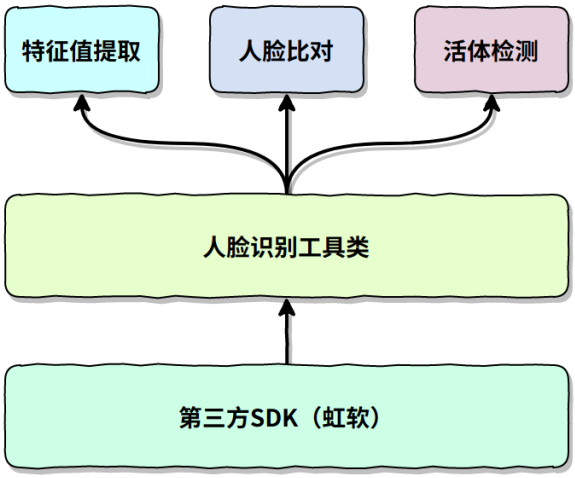


图 23 人脸识别

如上图所示，系统中所用到的关于人脸识别的相关功能依赖于第三方 SDK。根据

相关 SDK 开发集成了人脸识别工具。

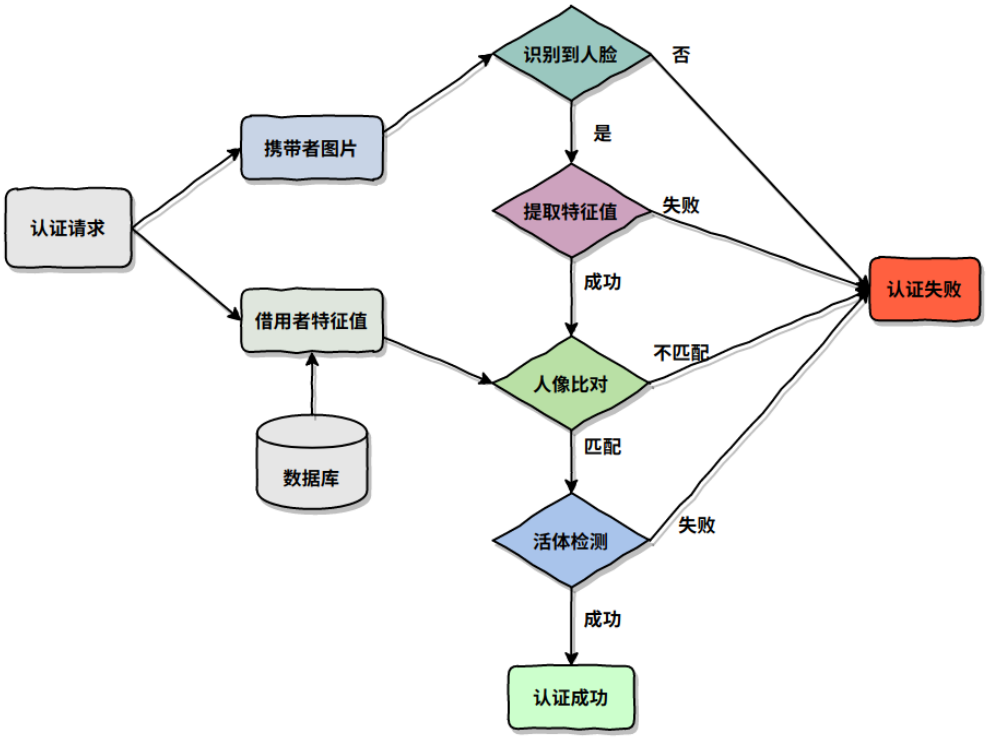


图 24 道闸处人脸比对流程

带出校验时需要进行严格的人脸比对，具体流程如上图所示：

- ✧ 当 RFID 探测器探测到重要设备或保密设备时，系统将发起人脸认证请求。
- ✧ 系统将道闸处摄像头拍摄到的照片传给人脸识别引擎，同时从数据库中读取该设备借用者（即有权限带出者）的人脸特征传给引擎。
- ✧ 引擎识别传入图片中的人脸，提取其特征向量，如未检测到人脸或特征向量提取失败则返回失败信息。
- ✧ 特征提取成功后，引擎将借用者特征向量与携带者特征向量进行比对，如相似度低于阈值则认为不是同一个人，返回人像不匹配失败信息。经试验，该项目中人脸比对阈值取为 0.80 时可获得良好效果。
- ✧ 如相似度高于阈值，则认为是同一个人，并对携带者图片进行 RGB 活体检测，防止人为作弊情况，例如携带者利用借用者照片迷惑人脸识别引擎。该项目中，活体检测阈值为 0.5。
- ✧ 如检测结果低于阈值，则返回非活体失败信息；否则返回成功信息，道闸处将放行。

3.3.3 数据库设计

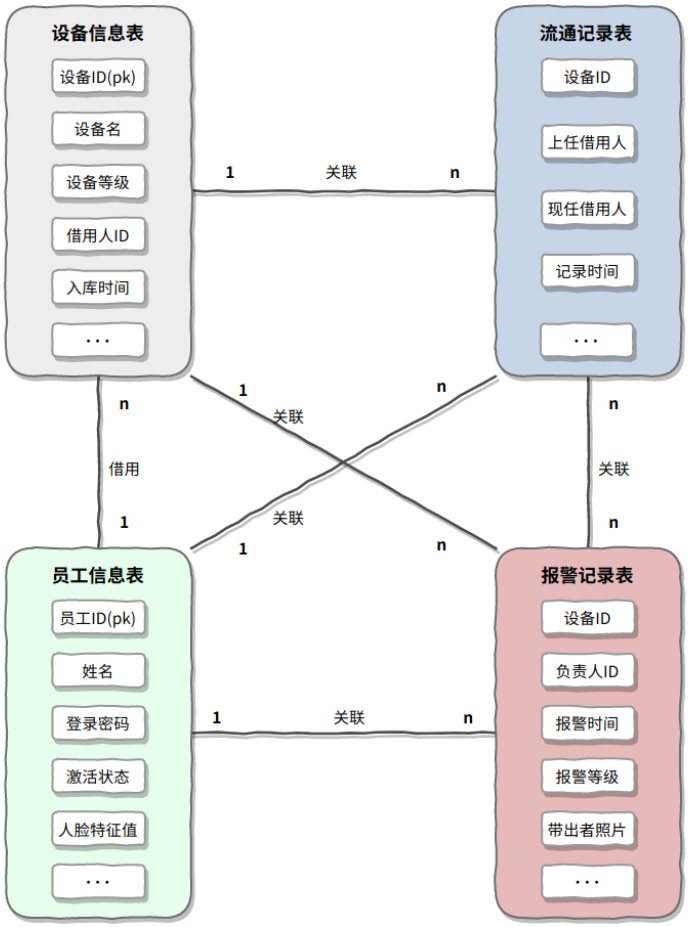


图 25 数据库关系表示意

如上图所示，该系统中主要建立了四张表，分别为设备信息表、员工信息表、流通记录表、报警记录表。下面就每张表的设计进行详尽阐述。

1. 设备信息表

表 3 设备信息表

字段	数据类型	描述
device_id(pk)	varchar	设备 id，nfc 芯片及二维码相同
device_name	varchar	设备名
device_level	int	设备优先级，及设备重要等级，（普通设备，重要设备，保密设备）
holder_id	varchar	负责人 id（为 NULL，则表示设备在库中）
create_time	timestamp	创建时间
update_time	timestamp	更新时间

该表用于存储系统所管理设备的相关信息，在上图所展示的字段中，着重阐述设备 ID、设备等级。

- ✧ **设备 ID**：前文对设备 ID 有过相关阐述，这里深入的解释在该系统设计设备 ID 的相关内容。
  - ➢ 获取方式：在该系统中，设备 ID 可以是设备出厂时烧录在相关芯片中的字符串，也可以是系统为其自动生成的 19 位字符串，只要能保证设备 ID 相对于系统所管理的设备唯一即可。
  - ➢ 绑定措施：当成功获取到某设备 ID 时，设备入库之前需要为该设备定制一张印有二维码的 RFID 芯片，该二维码所存储的数据为该设备 ID，该芯片存储的数据主要也是设备的 ID，当然芯片本身不是只能够存储设备 ID。二维码可以通过打印的方式动态生成，RFID 芯片可动态通过相关设备进行读写内容。简而言之，设备 ID、二维码、RFID 芯片三者是一一对应关系。
- ✧ **设备等级**：前文对设备分级也有过相关阐述，同样，这里深入的阐述为什么要将设备划分等级以及如何划分的。
  - ➢ 分级原因：在企业的需求中明确提到，需要对常规设备及重要设备进行相关管理，深入分析后，考虑到企业中的设备层级可能出现以下情况：
    - ◆ 即某些常规设备可由员工自由借还，并且当另一位员工需要该设备时，可以直接私下进行设备流通，只要遵循相关流通规则即可。此外，这些常规设备允许相关借用人员带出企业。
    - ◆ 某些设备可能存在一定的重要性，企业为了确保设备的安全性，可能会限制了该类设备带出。
    - ◆ 某些设备可能存在高度保密性，只有相关直接负责人能借用，并且该类设备不允许私下流通，每一次借还行为必须经设备管理员之手。
  - ➢ 设备等级：基于前面的三点分析，目前在该系统中主要设计了三种等级的设备，分别为常规设备、重要设备、绝密设备。相关内容在前文也有所赘述，这里再次分析不同层级设备的流通规则和带出限制。
    - ◆ **常规设备**：主要指企业中的工具类设备，比如一些鼠标、键盘。该类工具型设备允许员工自由借还，自由流通，同时允许员工将该类设备带出公司。
    - ◆ **重要设备**：主要指具有一定保密性质，但保密程度不高的仅用于开发设备，比如某合作企业提供的工程样机。该类设备允许员工自由借还、流通。但不允许该类设备带出企业。
    - ◆ **保密设备**：主要指公司研发的、需要保护其知识产权的等绝密设备，比如企业研发的带有特定功能的未加密保护摄像头样机。由于涉及到企业的知识产权，该类设备只能特定的人员进行借用，不允许内部流通，不允许带出公司。

2. 员工信息表

表 4 员工信息表

字段	数据类型	描述
employee_id(pk)	varchar	工号
employee_name	varchar	员工姓名
employee_gender	varchar	性别
employee_secret	varchar	登录密码（初始密码可自定义，若未定义则为 123456）
image_info	blob	人像特征信息（账号激活时需上传照片，通过人脸识别引擎获取）
active_tag	bool	激活状态
create_time	timestamp	创建时间
update_time	timestamp	更新时间

如上表所示，该表主要用于存储员工的相关信息，下面就其中的相关字段展开详细叙述。这里着重阐述表中的 **image_info** 字段。该字段用于**存储员工人像特征信息。**

在详细设计的人事管理小节中已经指出，当管理员在系统中导入人事表后，系统会为人事表中的员工创建一个未激活的账号，在员工登录这个账号开始使用相关功能前需要上传个人人脸照片进行账号激活。

所以，在该表中，image_info 是否存有该员工真实的人脸特征值就标志着该账号是否成功激活。

具体的激活流程在详细设计中人事管理小节也有详尽的叙述。即员工上传照片后，人脸识别引擎会提取该员工的人像特征值，并存储在数据库。

3. 状态变更记录表

表 5 状态变更记录表

字段	数据类型	描述
device_id	varchar	设备 id，nfc 芯片及二维码相同
pre_holder_id	varchar	上任负责人 id（为 NULL，则表示该记录为借出记录）
cur_holder_id	varchar	现任负责人 id（为 NULL，则表示该记录为归还记录）
create_time	timestamp	创建时间
update_time	timestamp	更新时间

如上表所示，该表存储的信息为设备状态变更记录，变更记录可以是设备借还记

录，也可以是设备私下流通记录。简言之，该表全面记录了设备相关状态变更所产生的信息。下面着重阐述关于 pre_holder_id 及 cur_holder_id 不同状况所对应的流通情况。

表 6 记录类型对照表

pre_holder_id（上任借用人 ID）	**cur_holder_id（当前借用人 ID）**	**对应记录类型**
NULL	NULL	\
NULL	非 NULL	借出记录
非 NULL	NULL	归还记录
非 NULL	非 NULL	内部流通记录

4. 带出报警记录表

表 7 带出报警记录表

字段	**数据类型**	**描述**
device_id	varchar	设备 id，nfc 芯片及二维码相同
holder_id	varchar	设备负责人 id
warn_level	int	报警等级，对应不同报警事件
carrier_photo_url	vharchar	携带者照片 url
warn_time	timestamp	报警时间
update_time	timestamp	更新时间

如上表所示，该表存储的信息主要为设备带出的相关报警记录。不同等级的报警记录对应着不同的设备带出情况。

表 8 报警记录带出情况对应表

报警等级	**报警类型**	**携带者 url**	**报警原因**
0	正常带出	NULL	正常合法带出
1	常规设备带出	携带者照片 url	携带者与借用者非同一人
2	非常规设备带出	携带者照片 url	重要或保密设备被带出
3	非常规设备带出	携带者照片 url	未登记借用设备被带出（**可定义为偷盗**）

3.4 用户侧

3.4.1 小程序扫码、扫 RFID 实现便捷借还

员工使用的小程序端页面路由结构设计如下：

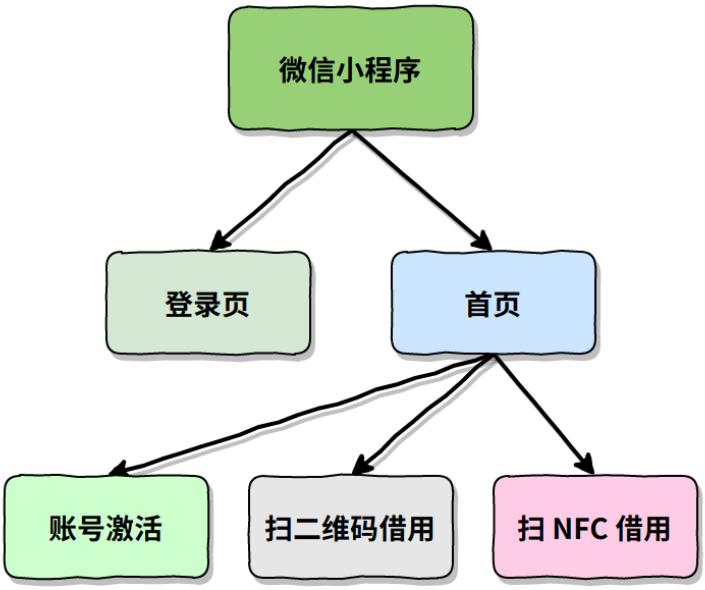


图 26 小程序页面路由结构

用户侧小程序实现便捷借还方案设计如下：

- ✧ 用户打开小程序，若为首次使用，则需要输入账号密码进行登录；若曾登录过，则使用微信开放平台提供的用户唯一认证标识 openid 与用户信息绑定，实现自动登录。
- ✧ 用户登录后，小程序端会根据当前账号的激活状态，展示用户对应可使用的功能：
  - ➢ 若账号**未激活**。用户账号未激活的情况下，首页将只显示一个功能——“账号激活”。在账号激活页面中，系统将引导用户修改初始密码，并上传个人照片，用于激活当前账号。
  - ➢ 若账号**已激活**。用户账号已激活的情况下，首页将显示当前用户的可用功能。小程序端可实现两个功能——“扫描二维码借用设备”或“扫 NFC 借用设备”。
- ✧ 用户选择任意一种方式进行设备借用时，首先会通过扫描设备二维码或扫设备 NFC 的方式获取到设备的 ID 值；其次，用户需要通过上文所述生物认证。两步完成后，即可实现设备的借用。

3.4.2 Web 管理系统实现设备高效管理

设备管理员使用的 Web 管理系统页面路由结构设计如下：

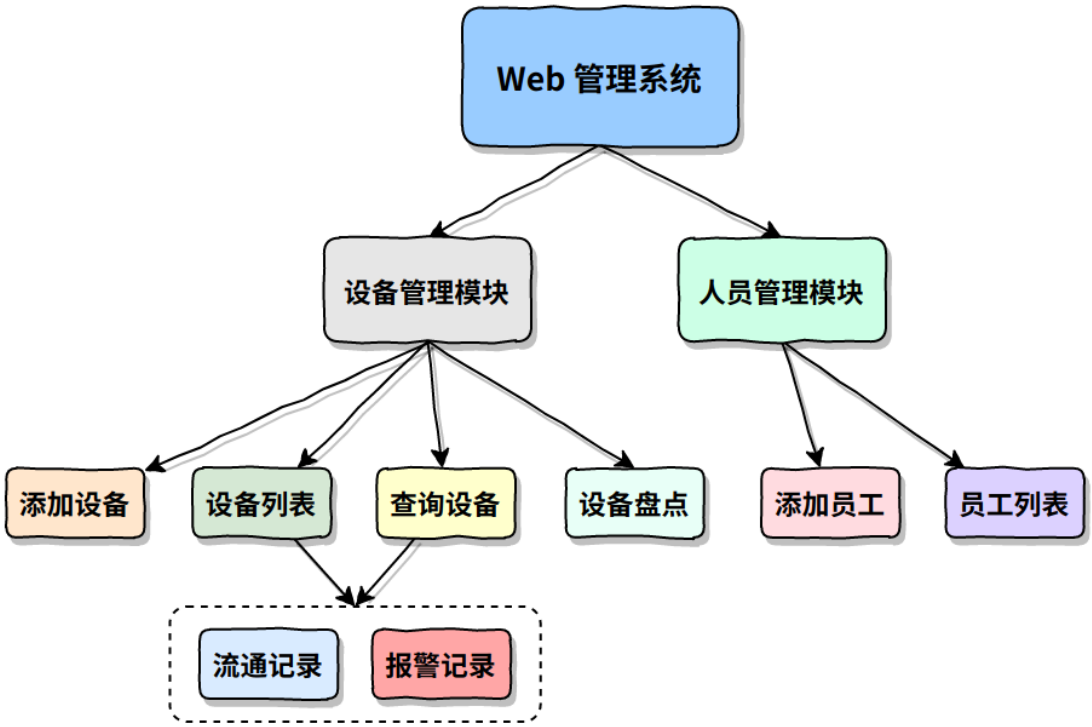


图 27 Web 管理系统页面路由结构

Web 管理系统提供给企业设备管理员使用，管理系统主要包含两个功能模块，其一是设备管理模块，另一个为人员管理模块。

设备管理模块中，设备管理员可对设备进行**设备入库、定期盘点、实时追踪**及**一键注销**等操作。

- **设备入库：**设备管理员可以创建包含设备信息的 Excel 文件，并通过上传指定格式的 Excel 表格文件的方式，批量快捷添加设备。
- **定期盘点：**通过设备列表查看所有设备，或通过查询设备页面，使用设备名称搜索设备，即可查看对应设备的流通记录以及报警记录。另有设备盘点页面使仓库设备概览信息一目了然。从而实现对设备出借、流转、带出、当前状态的实时便捷跟踪。
- **实时追踪：**该系统中，可查看所有设备列表或按设备名称查询到匹配的设备列表。
- **一键注销：**设备列表中可以对设备执行注销操作，针对不再需要管理的设备可以进行注销。

4 测试及运行效果

4.1 公司场景模拟

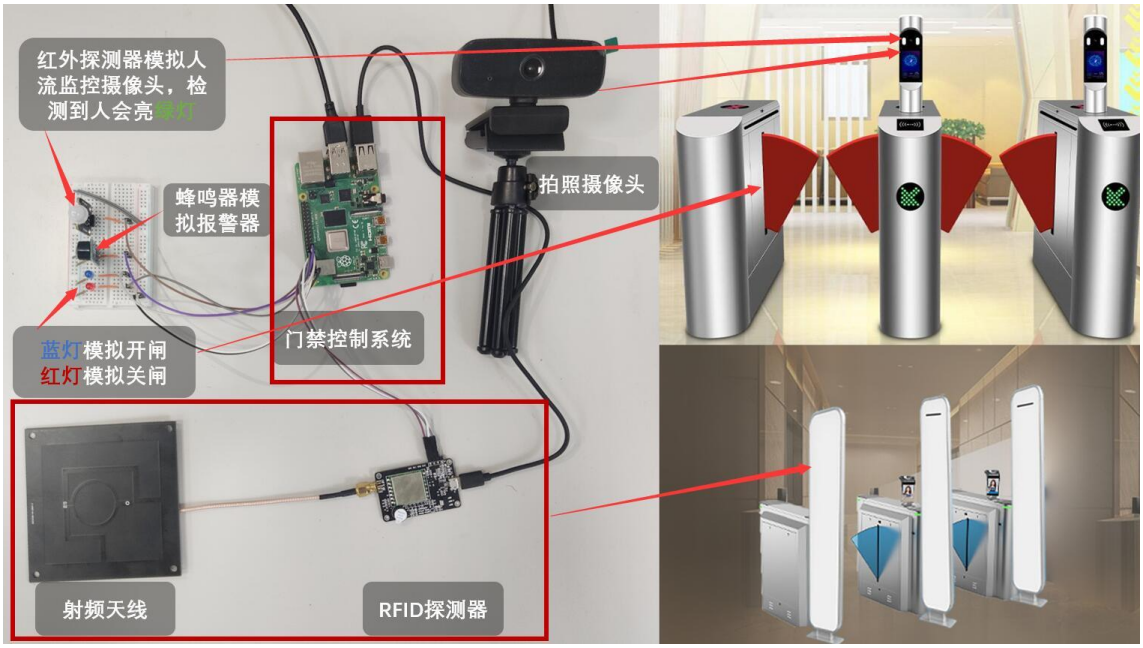


图 28 模拟场景示意图

如上图所示，模拟设备带出检测场景。

- ✧ 人体红外探测器：用于模拟人流检测摄像头，当检测到人流经过时，会亮绿灯，激活 RFID 探测器进行信号探测。
- ✧ 拍照摄像头：即上文所提到当 RFID 探测器探测到信号便会激活进行拍照的摄像头。
- ✧ 蜂鸣器：模拟报警系统。
- ✧ 发光二极管（蓝）：蓝灯亮，模拟放行动作。
- ✧ 发光二极管（红）：红灯亮，模拟禁止通行。
- ✧ RFID 探测器：被激活后，通过射频天线扫描一定距离内 RFID 标签

4.2 测试环境搭建

表 9 测试环境

	硬件配置	软件配置
服务器	小米 pro2019 CPU：i5-8250U 内存：8G 外存：256G	操作系统：windows 10 服务器：SpringBoot-2.4.4 内置服务器 数据库：mysql-5.5.40 Redis：redis-3.2.12 集成开发环境：IDEA
Web 管理系统	Dell G3590 CPU：Intel i5-9300H 内存：8G 外存：128G + 1T	操作系统：Windows 10 浏览器：Chrome 89.0.4389.128（64 位） 开发工具：Visual Studio Code
微信小程序	HUAWEI-YAL-AL00 CPU：Huawei Kirin 980 内存：8G 外存：256G	操作系统：Android 微信版本：8.0.2
门禁系统	RaspberryPi 4B+ 2GB UHF 超高频 RFID 射频模块 PCB 增益天线 USB 双目摄像头 人体红外传感器 有源蜂鸣器 示意 LED UHF 电子标签（普通、抗金属、抗高温）	操作系统：Raspberry Pi OS

4.3 运行效果

4.3.1 借还流程、内部流通运行效果

见附件演示视频。

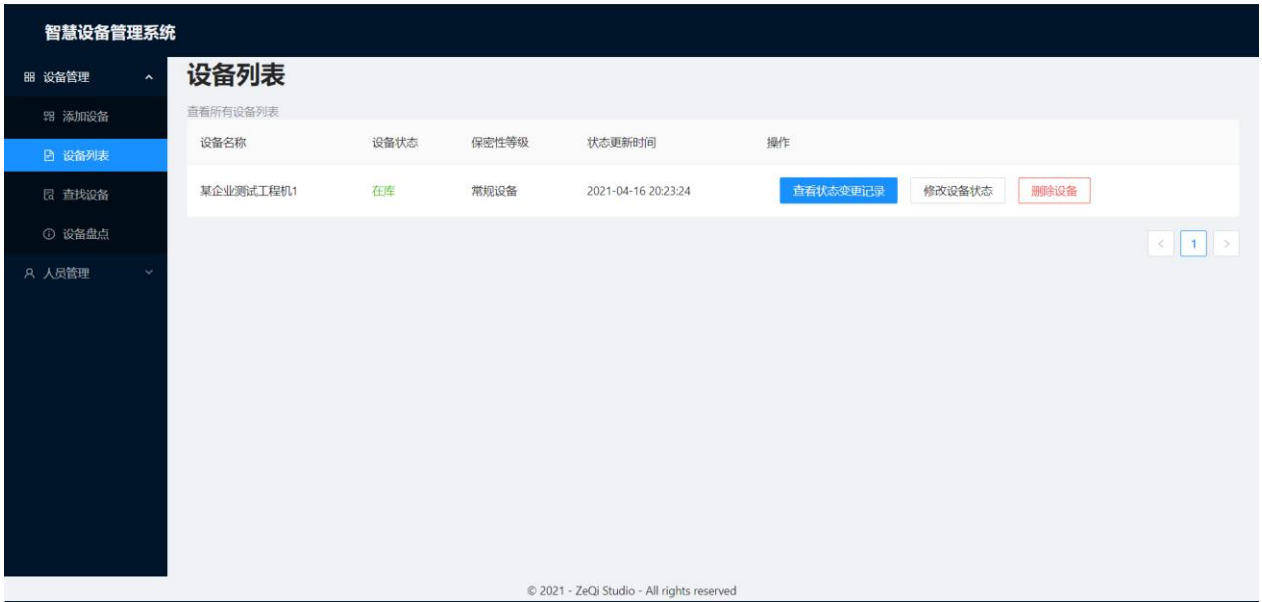
4.3.2 门禁系统运行效果

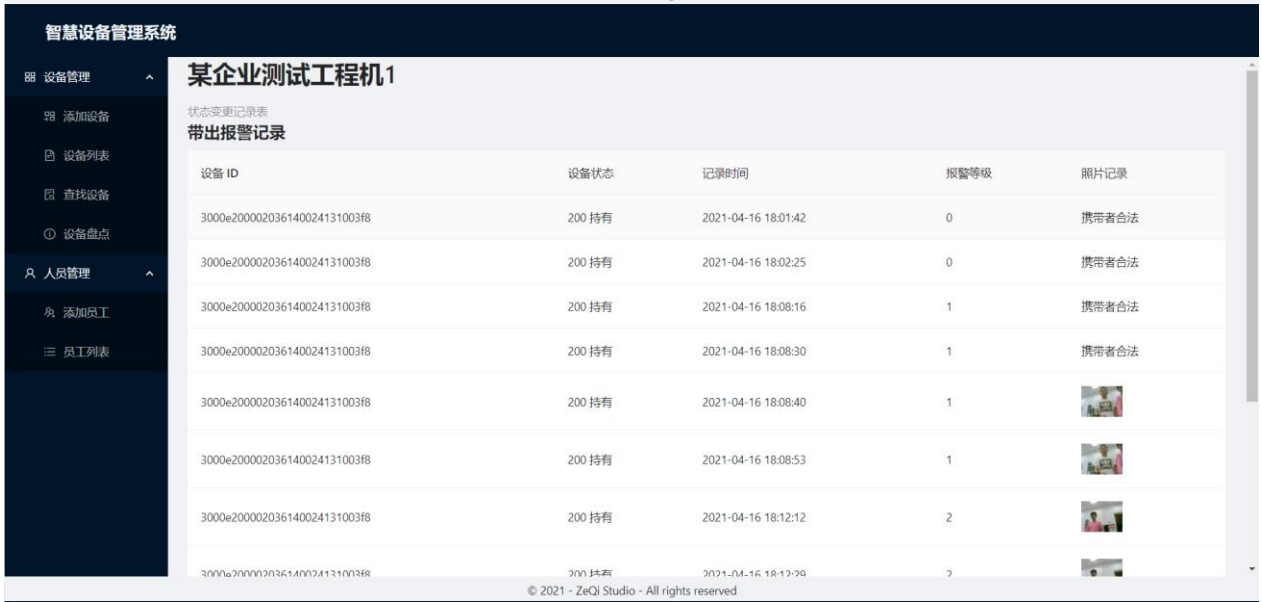
见附件演示视频。

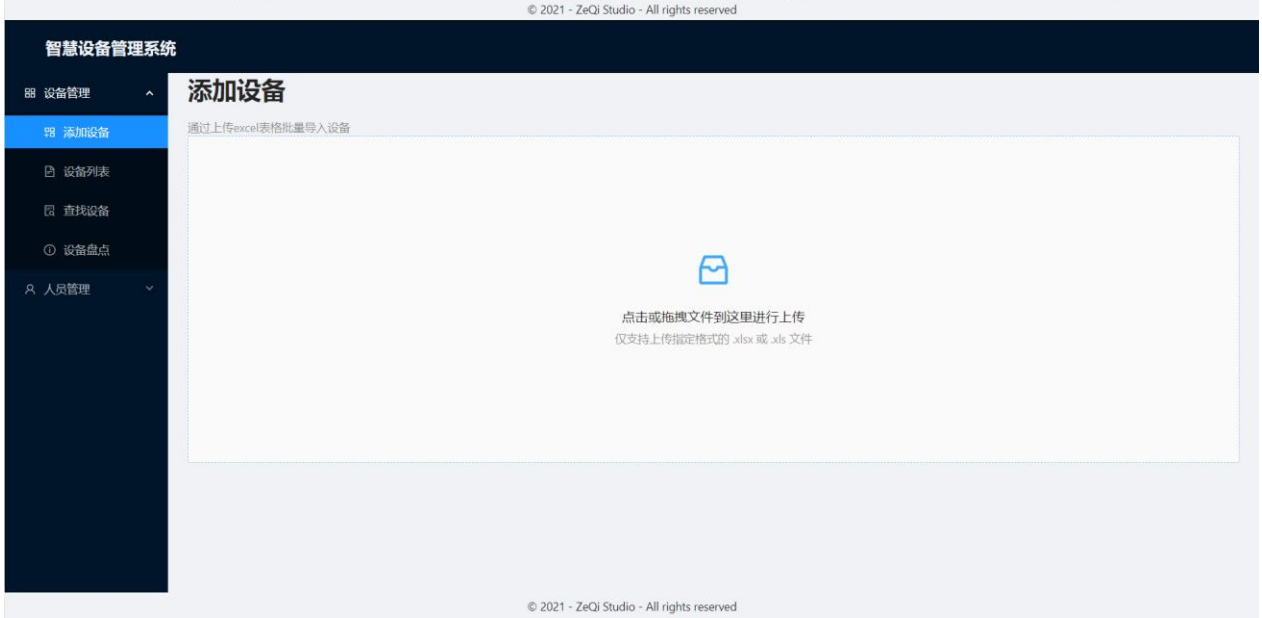
4.3.3 小程序运行效果

图 29 小程序运行截图

4.3.4 Web 管理系统运行效果







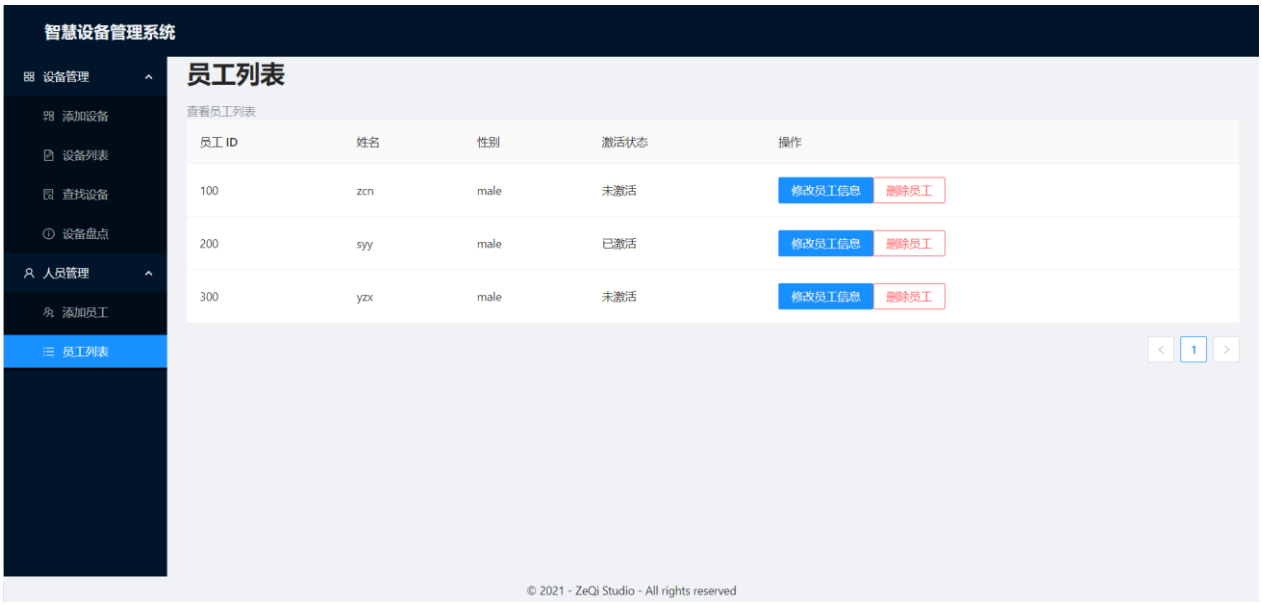


图 30 Web 运行截图

4.4 测试性能

表 10 性能测试表

测试项目	测试次数	系统平均响应时间 （检测到人流——给出放行结果）
不携带设备出闸机	50	0.61s
携带常规设备出闸机	50	2.80s
携带重要设备出闸机	50	2.12s
携带保密设备出闸机	50	2.09s

性能测试说明：

- **门禁控制系统**采用**树莓派**模拟真实场景的相关控制系统，在控制性能方面存在一定差距。
- **服务器**采用**个人电脑**搭建的本地服务器，与真实应用场景的高性能服务器相比，在认证性能方面也存在一定差距。
- RFID 探测器采用**低功率单模组**探测器模拟真实场景的**高功率多模组**探测器，在探测性能方面也存在一定差距。

5 创新与特色

5.1 设备全生命周期管理

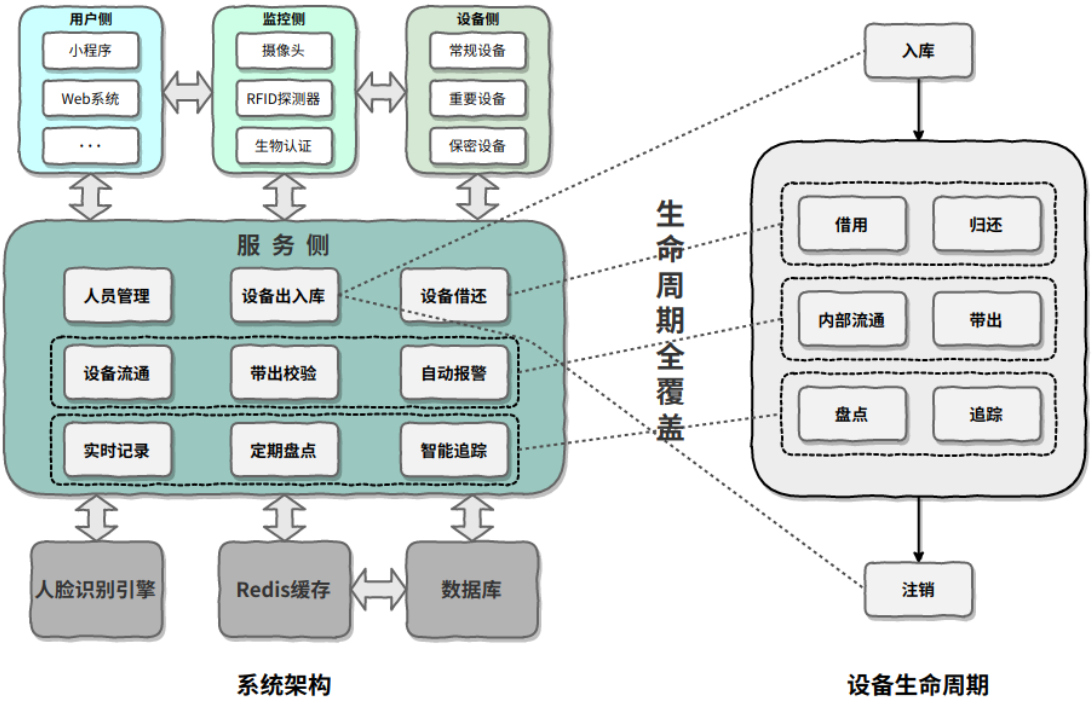


图 31 系统架构

如上图所示，该系统的设计覆盖了设备的整个生命周期。设备自入库起，经过长期的借还、流通，伴随着设备被带出公司，经过系统校验，以及期间的盘点追踪等管理流程，直至最终设备不再由系统管理，对设备进行注销，设备的整个生命周期都受到该系统的安全管理。

5.2 多维度便捷、安全流通策略

5.2.1 基于二维码、RFID 的便捷流通策略

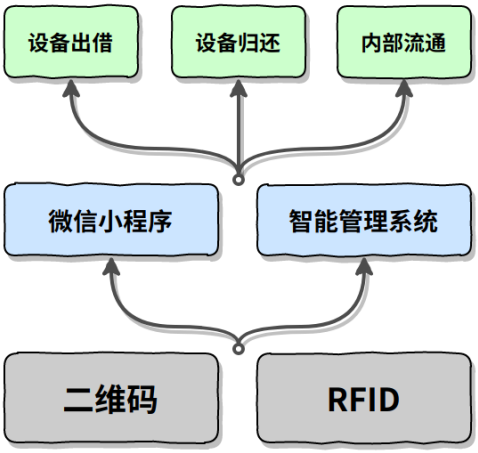


图 32 设备流通方案示意图

该项目设计中，每台设备上附有一张存储着设备信息的 RFID 芯片，面部印刷有二维码，用户通过微信小程序扫描设备二维码或 RFID 可完成设备借还等流程。

5.2.2 基于生物认证的防作弊策略

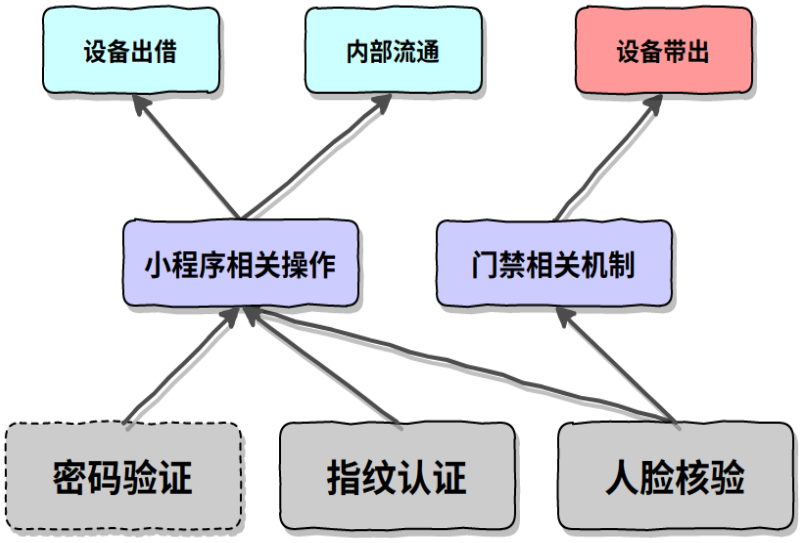


图 33 防作弊示意图

如上图所示，考虑到在设备流通过程中，二维码及 RFID 不具备用户识别功能，存在员工 **A 非法使用** 员工 **B** 的手机完成借用动作的可能性。针对此类情景，该系统对相关功能的使用采取了生物认证手段。在设备带出校验环节中，存在非法带出设备并使用**照片假扮真人**的可能性，在人脸认证方面也采取了**活体检测**相关手段。

5.3 设备非正常带出报警机制

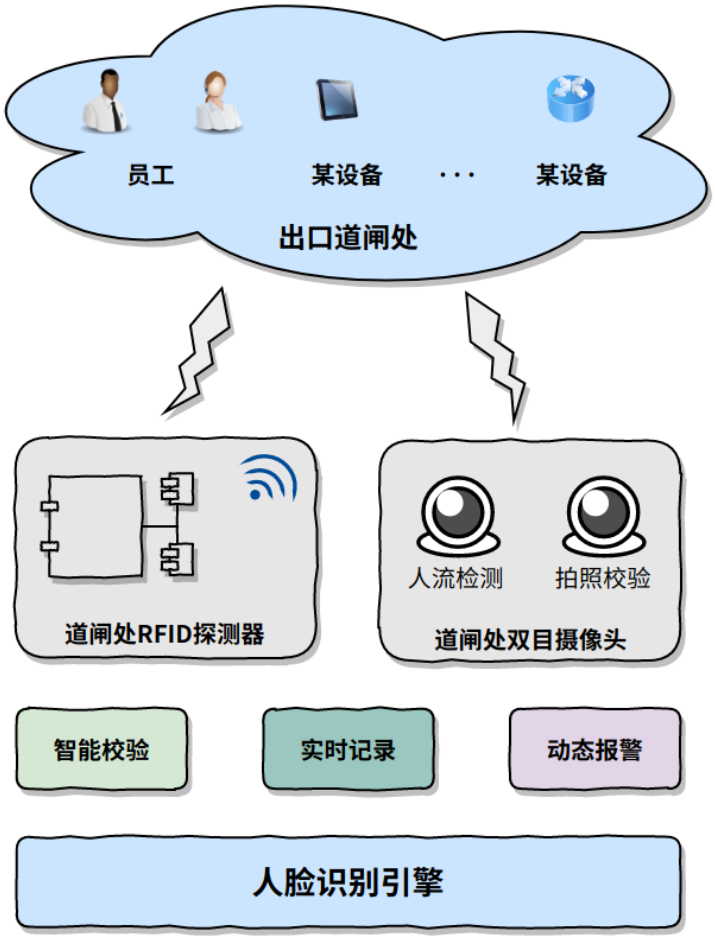


图 34 非正常带出报警机制示意图

5.3.1 基于 RFID 的高效探测手段

在公司出口道闸处安装 RFID 探测器，精准探测设备信号，及时捕获设备信息，确保每一台设备被带出都是合法行为。

5.3.2 基于人脸识别的合法性校验

安装 RFID 探测器的同时，也在合适位置安装高清摄像头，用于拍摄携带者照片，进行后续合法性校验。在上文中提到，该环节存在**人为作弊**可能性，进行人脸识别时会伴随进行**活体检测**，确保所拍摄的照片为真实人像。

5.3.3 非正常带出行为自动报警与记录

当设备被携带至道闸处时，会被系统检测到，通过摄像头拍摄携带者照片，并经过人脸识别引擎校验本次行为的合法性，采取相应的放行策略或报警机制，并实时记录非法人员人像信息。

6 结语

该项目聚焦企业设备高效管理，结合**人脸识别、RFID** 等创新技术手段，打造一套高效便捷的企业设备管理系统，解决设备管理存在的痛点，实现对设备入库、内部流通、设备借还、带出校验、定期盘点、实时追踪、自动报警等功能性需求的全面覆盖。兼具极强的**复用性**和**创新性**，同时具有极高的**使用价值**和**商业价值**。