机器人云端数据分时授信方法

机器人在不同时段，由于其作业的内容不同，所需要的数据也不同，我们希望机器人只有权限使用其作业时需要的数据，而对其他数据没有权限。我们设计了一套分时授信方案，来解决此问题。

按照排班表，设置证书的截止时间。

姓名：刘殿麒

联系方式：liudianqi@syriusrobotics.com

申请日期：20230626

专利申请部门： 智慧物联网开发组

主题：专利申请书

尊敬的专利申请部门，

我，刘殿麒，拟向贵部门申请下述发明的专利。我希望通过此申请获得专利保护，并提供以下详细说明以供审查。

- 专利申请的标题：
- 发明的概述：
- 详细说明：
- 参考资料：

专利申请的标题：

机器人云端数据分时授信方法

发明的概述：

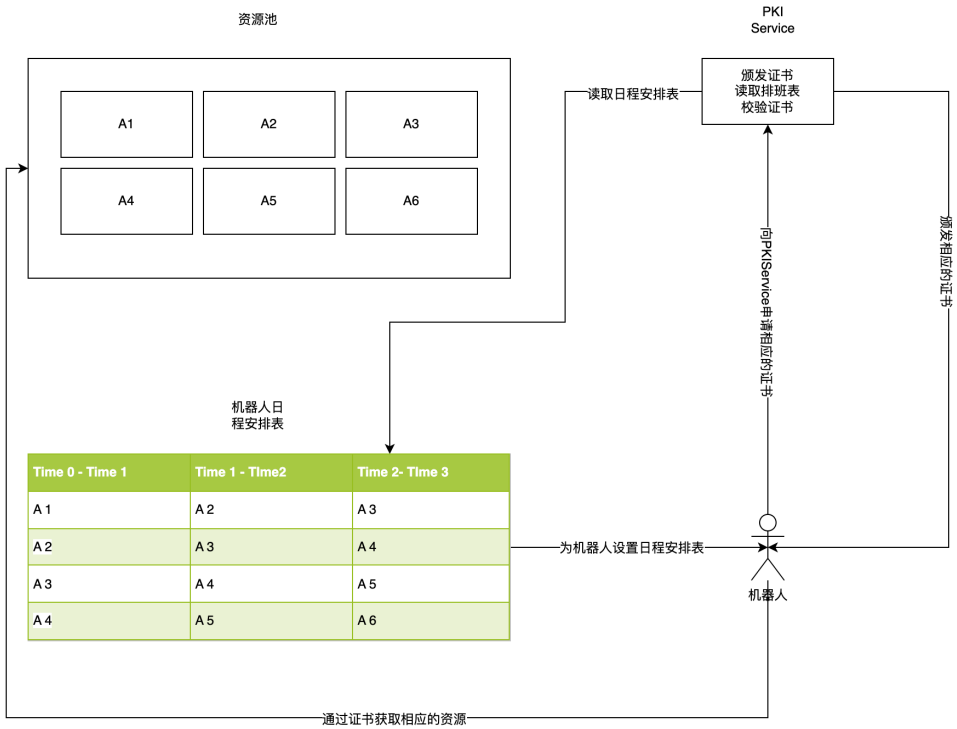
机器人在不同的时段有不同的作业内容，比如机器人在上午需要在仓库进行拣货业务，在下午需要进行每日新闻播放，机器人在上午只能获取到拣货任务的相关数据，比如拣货的订单/货物详情/货位号等相关信息，而在下午的作业中不希望机器人可以获取上午执行拣货任务时候所需的相关数据，比如场地的地图/拣货的订单/货物的详情等信息。

为了解决这个问题：

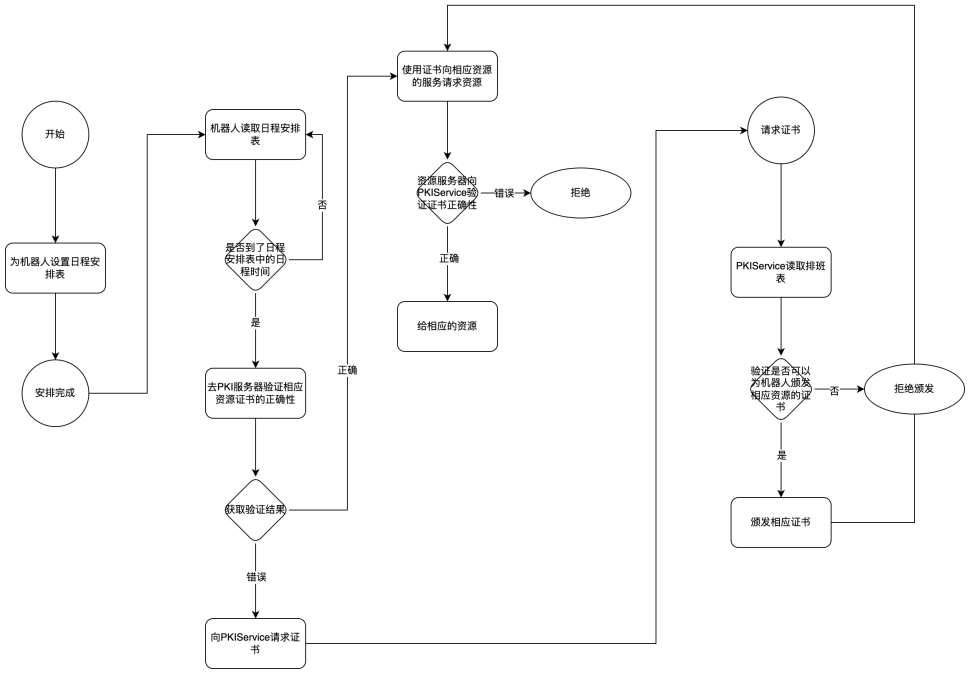
1. 首先需要为机器人设计一个【日程安排表】，这个【日程安排表】会标明这台机器人在某个时段【T<a>】所需要的资源(权限)集合【A1,A2,A3...,An】，即机器人的排班表为：T0:A1,A2...An，T1：A3，A4...,An，T2:A2,A3,...,An 。
2. A1对应着可以获得资源R1的权限，以此类推 An是可以获得资源Rn的权限
3. 有一个服务叫做【PKIService】，这个服务专门用来为机器人颁发可以拿到资源（权限）的证书，这个服务有所有资源（权限）【A<a>】的证书，这个服务可以读取机器人的【日程安排表】，并根据【日程安排表】的内容找到在当前时段【T<a>】该机器人所需要的资源（权限），然后为该机器人颁发获取相应资源（权限）的证书。
4. 相应资源的获取规则如下，需要机器人拿着有PKIService颁发的有效证书，去相应的权限服务器获取到权限然后拿着权限去相应的资源服务器获取资源。
5. 【PKIService】除了可以为机器人颁发的证书中存在以下的标识：
    a. 过期时间：expire time 过期时间表示该证书的过期时间，一旦过了过期时间该证书则无法通过PKIService 的校验，从而无法通过该证书获取到相应的资源（权限）
    b. 资源id： resource id，机器人可以通过该id获取到这个证书匹配的是哪个资源（权限）的证书
    c. 起始生效时间： start time，起始生效时间表示该证书从这个时刻起开始正式生效，在此之前 该证书依然无法通过PKIService的验证。
6. 机器人在要获取资源的时候拿着存在机器人中的证书向相应服务器请求相应资源，则可以获取到相应的资源一旦证书过期则无法从相应的服务器获取到新的资源。

详细说明：

1. 关系图：



2. 流程图：



参考资料：

X.509证书是一种常用的公钥基础设施（PKI）标准，用于在网络通信中进行身份验证和加密。在X.509证书中，有几个整数字段被使用。

下面是一些常见的X.509证书中使用的整数字段：

1. 序列号（Serial Number）：每个X.509证书都有一个唯一的序列号，用于标识该证书的唯一性。序列号是一个正整数。

2. 公钥指数（Public Key Exponent）：在证书中包含公钥时，公钥指数是用于加密和解密数据的指数。它通常是一个较小的素数。

3. 签名算法标识（Signature Algorithm Identifier）：用于标识签名算法的整数值。该值指示用于生成和验证证书签名的算法类型。

4. 版本号（Version Number）：用于指示证书的X.509版本。版本号通常是一个整数，例如0表示X.509v1，1表示X.509v2，2表示X.509v3。

5. 公钥长度（Public Key Length）：在证书中包含公钥时，公钥长度指示公钥的比特位数。它是一个正整数，表示公钥的强度和密钥长度。

这些整数字段在X.509证书的编码和解析中起着关键的作用，帮助确保证书的完整性和安全性。

PKI是公钥基础设施（Public Key Infrastructure）的缩写。它是一种基于非对称加密算法的体系结构和框架，用于管理和验证数字证书的创建、分发和撤销，以确保安全的通信和身份验证。

PKI系统通常包括以下主要组件：

1. 公钥加密算法：PKI使用非对称加密算法，如RSA、DSA或ECC，其中包括公钥和私钥。公钥用于加密数据和验证签名，私钥用于解密数据和生成签名。

2. 数字证书：数字证书是PKI的核心组成部分。它是一个包含公钥和相关身份信息的数字文件，由证书颁发机构（CA）签发。证书可以用于验证身份、加密和签名数据，以及建立安全通信。

3. 证书颁发机构（Certificate Authority）：CA是负责颁发和管理数字证书的权威机构。它验证证书申请者的身份，并使用自己的私钥对其公钥进行签名，以创建数字证书。受信任的CA可以构建信任链，使得证书的验证可以追溯到根CA。

4. 注册机构（Registration Authority）：RA是与CA合作的实体，负责验证证书请求者的身份，并将其身份信息提交给CA。RA在证书颁发过程中起到中间人的角色。

5. 证书存储库：证书存储库是用于存储和检索数字证书的集中式或分布式存储系统。它提供了公共访问点，以便验证方可以获取和验证所需的数字证书。

通过使用PKI，安全性和信任性得以增强，实现了以下目标：

- 身份验证：通过数字证书，PKI可以验证通信双方的身份，确保与合法和受信任的实体进行通信。
- 加密：PKI提供了加密算法和公钥交换机制，用于保护敏感数据的机密性和隐私。
- 数字签名：PKI可以使用私钥生成数字签名，验证数据的完整性和真实性。
- 数字证书撤销：PKI允许CA在需要时撤销数字证书，以确保无效证书不再使用。

PKI被广泛应用于安全通信、电子商务、远程访问和其他需要保证身份验证和数据安全性的领域。

AMR（Autonomous Mobile Robot）是一种自主移动机器人，被广泛应用于仓储和物流环境中的自动化操作。AMR仓储机器人具有以下特点和功能：

1. 自主导航：AMR使用激光导航、视觉导航或SLAM（Simultaneous Localization and Mapping）等技术，能够自主规划路径、避开障碍物，并在仓库环境中准确导航。

2. 智能任务执行：AMR可以执行多种任务，如货物搬运、拣选、仓储、装载和卸载等。它们可以根据仓库管理系统的指示，自主决策并执行任务，适应动态的物流需求。

3. 灵活性和可扩展性：AMR具有模块化设计，可以根据需要进行灵活配置和扩展。它们可以自主调度并协同工作，以适应仓库中的变化和不同的任务需求。

4. 安全性：AMR配备了传感器和安全功能，可以实时感知周围环境并避免碰撞。它们可以与人员和其他设备安全地共享工作空间，并具备紧急停止和安全保护机制。

5. 实时通信和监控：AMR可以与仓库管理系统或中央控制系统进行实时通信，传递任务状态和接收指令。管理人员可以通过监控系统追踪和监控AMR的位置、任务进度和性能指标。

AMR仓储机器人的引入可以提高仓库操作的效率、准确性和灵活性。它们能够减少人力需求，缩短物流周期，并提高库存管理的可视性和精确度。此外，AMR还能够适应快速变化的物流环境和需求，通过自主调度和协同工作，提供更高的生产力和客户满意度。