基于端云协同与联邦学习的多智能体机械臂协作系统

项目书

罗子昂[1]，李瑗蔚[2]，缪姝涵[3]

1 清华大学车辆与运载学院学院，中国 北京 100084

2 清华大学地球系统科学系，中国 北京 100084

3 北京大学人口研究所，中国 北京 100080

摘要：为提升智能机械臂系统在复杂任务中的泛化能力、协同效率与隐私保护水平，本文提出了一种融合端云协同架构与联邦学习机制的多智能体机械臂操作系统。系统采用云端大模型负责自然语言任务解析与任务拆解，端侧小模型负责具体动作执行，实现认知与执行的分工协同。在此基础上，系统引入联邦学习与知识蒸馏策略，支持各端模型在本地独立优化，保障数据隐私的同时提升整体任务泛化与模型个性化能力。本项目通过 AI2THOR 仿真平台对多任务、多设备场景进行测试，验证系统在动态环境中具备良好的鲁棒性与协同效率。技术创新包括：1）构建基于大模型 Agent 与联邦机制的端云协同框架；2）实现任务解析-执行流程的动态协同机制；3）利用联邦蒸馏提升系统泛化与模型定制能力；4）通过虚拟仿真验证系统在复杂环境下的可行性与实效性。本系统为构建面向真实场景的高适应性、多智能体机器人平台提供了新思路，具有广泛的工程应用潜力。

关键词：端云协同；联邦学习；多智能体系统；任务泛化；知识蒸馏；机械臂协作

目　录

1 项目背景与问题定义

1.1 应用背景

近年来，随着人工智能、物联网与自动化控制技术的持续突破，智能机器人逐步从实验室走向生产生活的各个角落，尤其在物流仓储、医疗辅助、工业制造、家庭服务等关键领域中发挥着日益重要的作用。根据《“十四五”智能制造发展规划》和工信部发布的《“十四五”机器人产业发展规划》，“到 2025 年，中国将建设 50 家以上智能制造示范工厂，机器人密度持续增长”，智能机器人已被明确列入国家制造强国战略重点方向。而在全球范围内，大国间围绕智能制造与机器人产业链的技术攻防与主导权竞争愈加激烈，已成为新一轮科技和产业革命的战略制高点之一。美国、德国、日本等发达国家相继推出“工业互联网”、“工业4.0”和“机器人新战略”等发展战略，中国则提出“智能制造+”、新型工业化、“以人工智能赋能传统产业”等举措，持续推动相关技术落地与规模化应用。

特别是在物流与仓储环节，随着电子商务与供应链系统的迅速扩张，企业对高效、安全、低成本、柔性强的智能化作业提出了更高要求。据中国物流与采购联合会数据，截至 2023 年，中国智能仓储设备市场规模已突破 2000 亿元，年均增长超过 20%。以京东、阿里、菜鸟、顺丰等为代表的头部企业已广泛部署机械臂系统实现自动分拣、搬运和打包等工作。然而，当前大多数机械臂系统仍采用“一个任务一种模型”的部署思路，即通过为每个固定任务设计专属控制逻辑与模型来执行，这种方式存在泛化性差、环境适应性低、部署与维护成本高的问题。面对日益复杂多变的作业环境和用户需求，这种刚性控制方式已难以满足对灵活调度与协同作业的要求。

在现实应用场景中，特别是仓储和制造业领域，一个典型任务往往由多个机械臂协作完成，例如，一台机械臂负责从货架取货，另一台机械臂将货物打包或移交给运输设备。这些任务不仅涉及对目标物体的准确识别与抓取，还常常面临动态障碍物、空间干扰、目标移动等复杂因素的挑战。在这种环境下，单一机械臂运行尚可控制，但一旦多个机械臂同时作业，传统基于静态规则或中心化调度的控制系统往往难以灵活适应。这不仅带来了碰撞风险和任务失败率的上升，也极大影响了整个系统的运行效率。

从学术研究与产业探索的角度来看，近年来机器人自主性与协同性的提升已成为国内外研究的热点。例如，斯坦福大学、MIT、清华大学、中科院自动化所等机构纷纷提出面向复杂任务的多智能体协作框架，尝试将人工智能大模型与端侧任务控制相结合，提高系统的泛化能力。同时，业界也在探索引入联邦学习机制，通过在保护隐私的前提下实现多端模型能

力的共享与提升，构建出更加智能、安全和可持续的协同系统。然而，目前已有研究在落地层面仍存在较大挑战。一方面，大模型虽然具备强大的理解与规划能力，但其部署成本高、资源依赖强，难以直接应用于算力有限的边缘设备；另一方面，小模型适配性强、响应速度快，但在面对新任务、新场景时往往缺乏足够的泛化能力。如何在两者之间建立高效协作关系，既发挥大模型在任务解析上的智能优势，又保留小模型在执行过程中的响应灵活性，成为突破现有瓶颈的关键方向。

更进一步地，随着国家对“低碳、智慧、高效”物流体系的重视，智能仓储、智能配送系统正在向更大范围、更高复杂度、更高协作度方向发展，对智能机器人的任务通用性、学习能力与协同控制水平提出了更高要求。这不仅是现有人工智能和机器人系统升级换代的“迫切需求”，更是未来十年产业蓝海的核心突破口。通过构建具备泛化能力、可自我优化、支持隐私保护的多智能体协作系统，有望填补当前机器人产业在“通用智能任务调度”与“端云协同优化”方面的空白，推动我国机器人技术从“点状替代”迈向“系统接管”，在全球技术博弈中抢占先机。

综上所述，当前智能机器人在关键行业的广泛应用为本项目的实践提供了现实需求支撑；而国家政策的支持与产业升级的需求，又为本项目的推进提供了有力保障。针对传统控制系统在任务泛化、环境适应性、隐私保护和多设备协作等方面存在的瓶颈，开发一种基于端云协同与联邦学习机制的多智能体机械臂系统，不仅是当前人工智能技术赋能机器人系统的关键方向，更是在新一轮国际竞争中实现技术突围、构建自主可控技术生态的重要探索。

1.2 当前挑战

当前，智能机器人技术尽管取得了阶段性进展，但在规模化应用和复杂场景落地的过程中，仍面临一系列亟待突破的关键难题。其中，**泛化能力不足、隐私问题以及多设备协作障碍**已成为制约其性能优化和部署扩展的三大核心挑战。

首先，**泛化能力不足**是制约当前机器人系统智能水平提升的首要问题。传统的机器人控制系统往往依赖于静态编程或单任务模型，即通过大量训练或规则设定，使系统适应某一特定场景或任务。例如，一个机械臂可以被训练得很好地完成某种特定物体的抓取任务，但一旦面对新的物体类别、工作台高度变化或空间布局调整，其表现便会迅速下降。这种模式本质上是“任务封闭式”的，一旦超出训练分布范围，模型就“不会迁移”，缺乏必要的泛化能力。用一句话来形容，就是“学过一个任务，换个环境或换种物体，就不会了”。这一问题在真实环境中尤为突出，因为机器人所面临的场景具有高度的开放性和不确定性。尤其在多任务、

多样化作业流程中，机器人需要具备跨任务、跨环境的理解与适应能力。因此，如何构建一种具有通用表达能力、可迁移、可组合的任务理解与执行机制，是目前亟需解决的关键难题。

其次是**隐私问题**。随着人工智能技术与机器人系统的融合，越来越多的智能终端部署于医疗、金融、家庭服务等涉及用户隐私的场景。这些应用通常需要大量个性化数据（如用户操作习惯、家庭布局、环境感知数据等）参与模型训练与优化。传统做法是将数据集中上传到云端进行统一建模，但这种方式存在极大的隐私泄露风险，尤其在涉及商业机密或个人敏感信息时。即使采用加密手段或匿名化处理，仍难以完全规避“重识别攻击”或数据重构风险。因此，如何在不暴露用户原始数据的前提下，实现模型能力的持续提升，成为关键技术瓶颈。联邦学习作为当前较前沿的解决方案，能够在“数据不出本地”的前提下，进行分布式模型训练，既保障隐私安全，又实现跨用户泛化。这一机制尤其适用于智能机器人系统的部署场景：不同用户的环境、任务和需求各异，如果每台设备都“只学自己那一套”，系统就无法演化出更强大的通用能力；而通过联邦学习，可以在保护隐私的前提下实现模型间的知识共享与协同进化，从而突破“个体训练-难以泛化”的困境。

第三个亟待突破的挑战是**多设备协作障碍**。随着机器人从单机作业向多机械臂、多智能体系统演化，复杂任务往往需要多设备协同完成。例如，在仓储物流中，一项任务可能涉及不同位置的抓取、分拣、搬运与装载等多个环节，往往由多台机械臂同时执行。此时，若缺乏良好的任务分解、路径规划和执行协调机制，极易出现重复操作、冲突甚至物理碰撞，严重影响系统整体效率。当前主流的多机器人调度系统多基于中心化的静态规则制定，不具备实时自适应能力。当系统规模扩大或作业任务增多时，调度瓶颈尤为明显，容易造成响应延迟和资源浪费。更严重的是，传统系统往往以单个机器人为最小单位进行优化，忽视了智能体之间在空间感知、状态共享和策略协同上的需求，无法形成真正意义上的“群体智能”。多设备协作的本质不只是“并行执行”，而是“协同规划、动态响应”，要求每个智能体在了解自身状态的同时，能够感知并预测其他机械臂的动作，进而实现任务间解耦、空间上避让和执行节奏协调。

综上所述，这些挑战之间并非孤立存在，而是彼此交织、相互强化：任务泛化能力不足，会导致协作僵化、调度不灵活；缺乏隐私保护机制，会限制多终端之间的知识共享；而协作机制的薄弱，则会放大模型能力差异，进一步压缩系统泛化空间。因此，如何统筹解决泛化能力、隐私安全与协同调度的问题，构建一个既智能、高效，又具可扩展性和可部署性的多智能体机器人系统架构，是当前人工智能赋能实体机器人系统最具挑战性、同时也最具潜力的研究方向之一。

1.3 核心问题

首先，如何**在动态环境下保证多机械臂系统的任务泛化能力**，是实现多智能体系统规模部署与持续适应的基础。多机械臂协作系统通常部署在结构复杂、任务多变的场景中，如智能仓储、柔性制造、家庭服务等。这些场景具有典型的非结构化特征：目标物体类别不固定，空间布局实时变化，任务指令具有自然语言表达的开放性。要让系统具备应对这些变化的能力，必须引入具备通用感知与规划能力的模型结构。本项目拟采用大模型驱动的任务理解与规划机制——通义千问 Qwen2.5-VL-32B-Instruct 具备跨模态理解能力的指令大模型，在云端完成对自然语言任务的语义解析、意图建构与高层任务规划；并将其输出的任务拆解（planning）结果下发至端侧小模型执行。大模型可基于少量提示学习、上下文增强推理，实现复杂任务指令的快速解析与子任务生成，从而赋能小模型具备“见所未见”任务的适应能力。在此基础上，端侧小模型再结合视觉输入和传感器反馈，实现路径动态调整与操作落地，从而构建起一个具备高泛化性、强任务适应力的“感知—规划—执行”一体化体系。

其次，如何**通过联邦学习技术，在隐私保护前提下实现模型能力迁移与共享**，是提升系统智能性与用户信任度的关键。多机械臂系统在不同用户或不同场景中部署，其操作对象、任务习惯、环境结构往往存在较大差异，因此单一模型无法覆盖所有边界条件。与此同时，用户对数据安全和隐私的敏感性也越来越高，特别是在家庭服务、医疗护理、企业操作等应用场景中，要求设备不能将本地数据上传至云端。在此背景下，联邦学习（Federated Learning）提供了一种兼顾性能与隐私的训练范式：各端侧模型在本地利用各自任务数据进行自主优化，不上传原始数据，仅共享模型权重或参数更新，云端通过周期性聚合与蒸馏，更新全局模型并反馈至各端设备。这一机制不仅避免了隐私泄露风险，还能实现跨设备、跨用户的能力迁移与泛化。在本项目中，我们将设计专用于多机械臂的联邦优化流程，结合任务类型标识、环境上下文信息、设备算力情况等元信息，引入个性化聚合策略，以实现“共性抽取 + 个性保留”的模型协同优化过程。这将打破当前端模型“只能学自己的数据，学不来别人的经验”的限制，为多机械臂系统提供持续演化的认知能力支撑。

最后，如何**基于端云协同的大小模型技术，实现多机械臂的高效协同**，是保障系统整体执行效率与可扩展性的关键所在。在传统机器人控制系统中，任务执行与控制逻辑多为单体构建，机械臂之间缺乏高效的通信机制与协同策略，一旦任务流程复杂或空间重叠，便容易出现动作冲突或资源竞争，进而影响系统稳定运行。为此，本项目提出基于“端云协同 + 多智能体分布控制”的架构设计思路：云端的大模型负责全局任务感知、任务分解与协同规划，

而端侧小模型则根据自身状态与接收任务，自主进行路径规划、动态避障与进度反馈。不同机械臂之间可通过轻量化通信协议实现状态感知与协同决策，使整个系统具备“集中理解—分布执行—协同协调”的功能闭环。此外，借助联邦学习机制，各端模型在独立执行过程中还能学习到其他机械臂的操作策略，通过云端知识融合进一步提升协同效率。最终构建起一个具备高并发、高协调性、高稳定性的多机械臂协作系统。

任务泛化能力、隐私保护与协同执行效率三者构成了智能机器人系统向更高级阶段发展的技术支柱。本项目围绕这三点展开系统性创新，目标是在真实环境中建立起一个具备自主理解、隐私自守、协同进化能力的端云一体化多智能体机器人操作系统。

2 项目目标与设计理念

2.1 项目愿景

本项目旨在构建一个具备任务泛化能力、隐私保护机制与多智能体高效协作能力的下一代机械臂操作系统。该系统能够适应动态变化的环境与任务需求异构化趋势，在复杂、多变的操作场景中保持稳定、高效的执行表现。特别是在多物体、多障碍物密集环境中，系统应能够实现精确的目标识别、智能路径规划与灵活的协同抓取。此外，系统将依托大模型与小模型的分层协同机制，实现从任务理解到动作执行的全流程智能调度，提升系统整体的响应速度与操作精度。

在现实应用中，机械臂不仅仅执行重复性的动作，更需要面对高度变化的任务需求和环境扰动，例如电商仓储中的动态分拣、工业生产中的装配变更，或医疗场景中的个体差异化手术支持。这些场景对机器人系统提出了更高层次的智能要求，传统的基于规则的自动化系统在适应性与泛化能力上存在明显瓶颈。本项目希望通过融合大语言模型的任务理解与联邦学习的个体适配能力，打破现有系统在环境适应、任务迁移与隐私处理方面的技术限制，为未来智能机器人操作系统提供新范式。

最终目标是：打造一个面向未来复杂环境、支持多任务、多设备协同操作的机器人平台，具备从理解自然语言任务意图、到自主规划与高效执行的闭环能力，同时确保在数据不出本地的前提下实现能力迁移与模型共享。

2.2 总体设计思想

为实现上述目标，本项目提出了“三层协同、双重优化、动态适配”的总体设计思路，围绕大小模型协同、联邦学习与任务多样性适应三大核心机制展开。

2.2.1 大小模型协同：云端智能规划+端侧敏捷执行

系统采用云端-端侧协同模型架构，将复杂任务的解析与拆解交由云端大模型处理（Qwen2.5-VL-32B-Instruct 具备语言-视觉推理能力的模型），将具体动作执行与环境感知交由端侧小模型完成。

云端大模型负责从自然语言任务指令中提取关键语义信息，执行高层次的任务解析、意图识别与子任务规划，并根据全局状态协调多个机械臂的子任务顺序与资源调度。相比之下，小模型则部署在每台机械臂本地，负责执行细粒度的任务动作，如抓取、移动、避障、反馈等操作。二者通过低延迟接口通信完成动态配合，确保系统在面对复杂环境时既具备战略层

面的智能判断能力，又具备战术层面的快速执行反应能力。

这种“大脑+神经末梢”式架构不仅提升了系统的任务解析能力，也保障了在终端资源有限情况下的执行效率，最大程度平衡了全局智能与本地反应能力之间的矛盾。

2.2.2 联邦学习机制：在隐私保护中实现能力共享

为了保障系统的可扩展性与用户隐私，本项目引入联邦学习机制（Federated Learning），使每个端侧设备（小模型）能够在本地完成模型更新和任务优化，而无需将原始数据上传至云端。云端通过定期收集模型参数或梯度信息，使用联邦平均聚合算法与模型蒸馏技术进行统一优化，并将优化后的全局模型反馈至各终端，实现模型间的知识共享与能力迁移。

在该机制下，每个小模型不仅能够根据其本地任务、环境与偏好进行个性化训练，还能借助系统中其他设备的经验不断演进，从而在不牺牲隐私安全的前提下，逐步提升整个系统对多任务、多场景的适应能力。这种“学习在本地，成长在全局”的方式，尤其适合需要部署在医疗、家居、金融等对隐私保护高度敏感的场景中。

2.2.3 任务、多设备、多环境：全流程动态适应机制

为进一步提升系统在真实世界复杂环境下的实用性，本项目从设计之初即面向多任务、多设备、多环境适应性的需求，构建了可扩展、可迁移、可自适应的调度与控制机制。

在多任务方面，系统支持异构任务混合编排与子任务重构，可将复杂任务拆解为多个操作模块，并动态组合执行路径；在多设备方面，系统可根据机械臂的能力分级与空间位置，采用分布式任务调度算法实现最优资源匹配与冲突规避；在多环境方面，系统具备实时感知与反馈机制，能够自动调整动作策略，在遇到新目标、障碍物或执行失败时，触发局部replanning，从而保障任务的稳健执行。

此外，系统还支持通过历史反馈学习机制，对任务执行数据进行结构化编码，用于优化后续任务的策略选择与路径生成，构建真正意义上的“数据驱动任务调度器”。最终实现一种具备自适应、自协同、自演化能力的智能机器人协作系统架构。

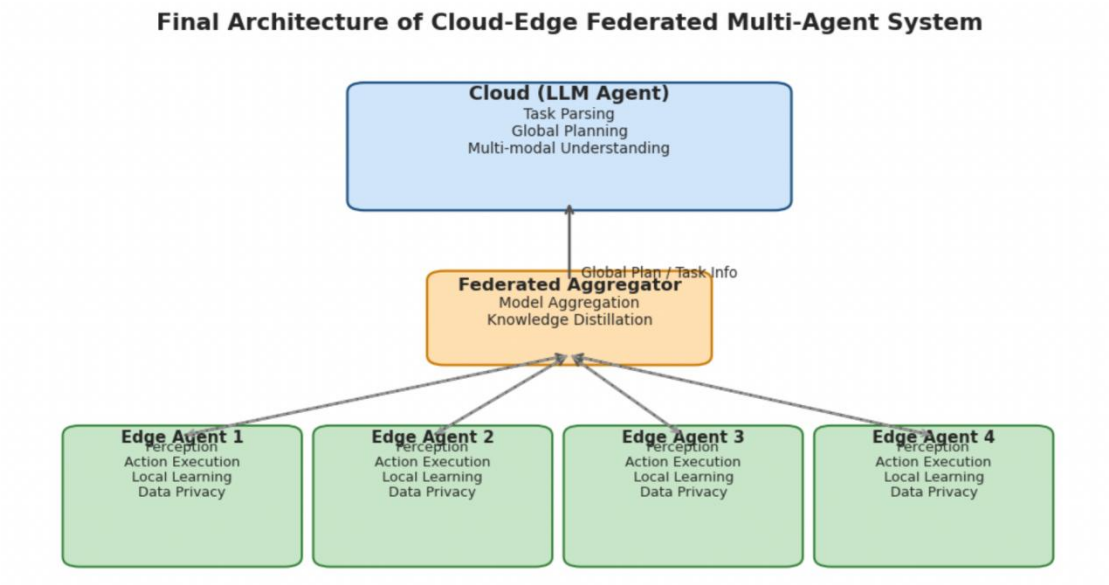

图 1 系统逻辑架构图，包括云端（Cloud Side）、联邦学习机制（中间层）、端侧（Edge Side，多个端臂）

3 系统架构与关键模块

3.1 系统总体架构图

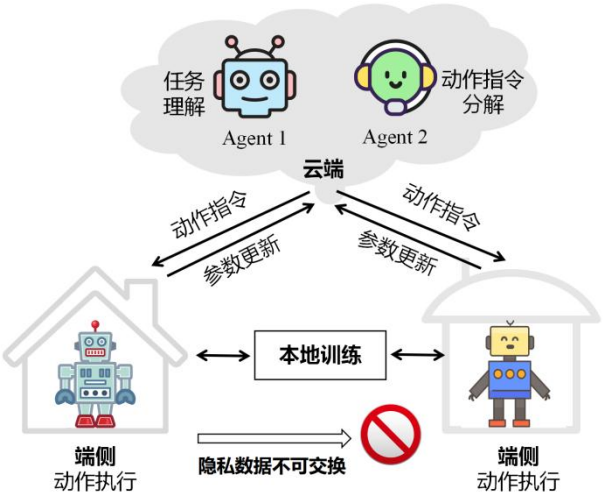

图 2 系统总体架构图，

本系统的架构基于端云协同和联邦学习的结合，通过云端与端侧的协作，形成高效的任务执行和数据隐私保护机制。云端的任务解析与规划能力与端侧的小模型执行能力相结合，形成一个智能、高效且可扩展的系统架构。系统架构图展示了云端与端侧的分工和信息流动，其中云端负责高层任务的解析与分配，而端侧小模型则负责具体任务的执行和反馈。联邦学习模块则在整个过程中保障隐私保护并实现系统优化。

3.2 云端模块（大模型智能体）

在本系统中，云端模块的核心任务是进行高层任务理解与规划。云端模块通过两个智能体（Agent）来分别完成任务理解与子任务规划。

3.2.1 任务理解（Agent 1）

云端的第一个智能体，Agent 1，负责解析用户的自然语言指令。用户通过自然语言向系统发出指令，例如“将桌上的杯子搬到架子上”。Agent 1 会首先理解任务的意图，识别任务目标，并将其转化为系统可以处理的指令。通过使用大模型，如基于深度学习的自然语言处理（NLP）模型，Agent 1 能够有效地理解任务中的复杂语义，并能够识别出执行任务所需要的具体动作和条件。

3.2.2 子任务规划（Agent 2）

云端的第二个智能体，Agent 2，负责将任务拆解为具体的子任务。这些子任务是机械臂可以执行的具体动作，例如“移动到桌子前”，“抓取杯子”或“将杯子放到架子上”。通过任

务拆解，Agent 2 能够根据任务的复杂程度和实际环境条件，设计出合适的执行路径，并将这些子任务指令发送给端侧的小模型。每个子任务不仅包含动作指令，还会包含环境信息、限制条件等，用于指导小模型如何在复杂环境中执行。

3.3 端侧模块（小模型执行器）

端侧模块的核心任务是执行云端下发的任务指令，并提供实时的执行反馈。端侧小模型的设计重点是如何在实际操作中实现高效的动作控制和精准的目标识别。

3.3.1 动作控制

端侧小模型根据云端的指令执行具体操作。这包括根据云端下发的任务目标，调动机械臂进行物体抓取、移动或放置等操作。每个小模型专注于局部任务的执行，如物体的抓取与释放、避障路径的规划等。端侧小模型通过传感器实时获取周围环境的变化，并结合实时数据调整操作策略，确保任务高效且精确地完成。

3.3.2 对象识别与反馈机制

为了确保操作的准确性，端侧小模型还包括了对象识别功能。通过安装的视觉传感器或摄像头，小模型能够实时识别操作环境中的目标物体，并进行位置定位。在物体抓取的过程中，计算机视觉算法帮助小模型识别目标物体的具体位置与状态，从而确保机械臂能精确抓取到目标。同时，执行过程中，小模型会将其状态和操作结果反馈给云端。这些反馈信息不仅用于云端对当前任务的优化，也能为后续任务的执行提供参考。

3.4 联邦学习模块

联邦学习模块的加入，使得本系统能够在保障用户数据隐私的前提下，充分利用各端模型的数据进行集体优化。通过本地训练和模型聚合，本模块确保每个端侧小模型能够在其本地数据上进行优化，同时提升系统整体的智能水平。

3.4.1 客户端本地训练

在本系统中，端侧小模型并不直接上传其本地数据到云端，而是在本地使用自己的数据进行训练。这一设计能够有效保护用户的隐私数据，如医疗数据、用户行为数据等，避免数据泄露或滥用。每个端模型根据自己的执行环境和任务数据进行训练，不同的端侧模型能够学习到不同的执行策略和应对环境变化的能力。通过这种方式，系统可以在不同环境和任务中进行灵活的学习和调整，确保每个机械臂都能根据本地情况进行有效的执行。

3.4.2 模型聚合与蒸馏流程

尽管每个端模型在本地训练，但它们仍需通过联邦学习的聚合机制进行协同优化。云端定期从各端模型收集更新后的参数，并通过模型蒸馏等方法将各个端模型的知识进行融合。这种聚合不仅能够提升每个端模型的性能，还能通过全局优化，提升系统的整体能力。例如，云端模型可以提取各端模型的优质特征，并传递给所有端模型，确保每个端模型都能学习到其他端模型在不同任务和环境中的优势。通过这种协作机制，系统能够不断自我优化，在多任务、多环境的场景下实现更高效的执行。

4 技术实现路线

4.1 核心方法与参考模型

在本项目中，我们将采用 VoxPoser 和 CROSSLM 的联邦机制作为核心技术方法，确保系统能够高效执行任务并持续优化。

4.1.1VoxPoser

VoxPoser 技术是我们任务解析和轨迹生成的核心工具。它通过结合云端大模型的任务解析能力和端侧小模型的具体执行能力，为机器人提供了精准的轨迹规划。这一技术的独特之处在于，VoxPoser 利用 3D 价值图来表示任务中的空间约束和目标位置。通过这种三维图形表示，系统可以准确地了解任务中的物理目标，并对路径进行优化。例如，在执行一个抓取任务时，VoxPoser 会生成一个三维价值图，指示机器人抓取目标物体的位置、需要避开的障碍物，以及如何优化运动路径来避免碰撞。

此外，VoxPoser 不仅能通过生成的价值图来指导机器人如何规避障碍，还能动态地生成适应任务变化的轨迹。这意味着当环境或任务条件发生变化时，机器人能够实时调整其动作轨迹，以应对新的挑战，从而提高任务执行的效率与精度。这种灵活的轨迹规划能力特别适用于复杂的、多变的工作环境，使得机器人能够在没有固定规则的情况下，灵活应对不同的任务和环境。

通过代码生成与三维价值图的结合，VoxPoser 不仅能够完成任务的解析，还能根据解析结果实时生成适合执行的路径。这种基于任务需求和环境变化进行动态调整的机制，使得系统能够在多变的环境中维持高效的执行能力。与传统的基于静态规则的执行方式相比，这种方法具有显著的优势，能够提供更高效、灵活且智能的解决方案。

4.1.2CROSSLM 的联邦机制

为了解决隐私保护问题并优化系统的执行效率，本项目采用了 CROSSLM 的联邦机制。该机制通过大模型与小模型之间的知识共享与互相促进，有效提升了系统的泛化能力与执行效率。具体来说，CROSSLM 框架首先在云端部署一个强大的大模型，负责任务的解析和子任务的规划。大模型在处理任务时利用其深厚的知识库，能够对复杂的任务进行精准的分析与分解。

与此对应，端侧的小模型负责根据云端指令执行具体的任务。这些小模型在本地根据自己的任务和数据进行训练，优化执行策略，但并不需要将用户的敏感数据上传到云端，从而实现隐私保护。这些小模型通过在本地不断积累经验和知识，能够根据不同的任务环境做出

更加灵活的反应。

云端模型则通过定期的模型聚合过程，将各个端模型的训练成果汇总。通过模型蒸馏等技术，云端能够将各端模型的优质知识和经验提取出来，汇总进全局模型中，进一步提升系统的整体性能。这种联邦学习机制不仅保证了隐私保护，还能够有效提升小模型的执行能力和适应能力，使得系统在执行多样化任务时能够表现得更加高效和精准。

4.2 任务流程示意图

本系统的任务执行流程通过自然语言指令的解析与多层次任务拆解来实现。具体的任务流程如下：

首先，用户通过自然语言输入任务指令，例如“将桌上的杯子放到架子上”。这一指令会被传送至云端模块，由云端的大模型进行解析。通过强大的自然语言处理（NLP）能力，云端大模型能够理解用户的任务意图，并识别任务目标。这一过程是任务执行的起点，也就是自然语言指令 → 云端解析。

接着，云端的大模型将任务解析成多个具体的子任务。这些子任务细化为机器人可以执行的操作步骤，例如“移动到桌子前”，“抓取杯子”，甚至“避开障碍物”。任务拆解的核心目的是将复杂任务转化为多个可执行的子任务，这样不仅有助于提升任务执行的效率，还能够减少因任务复杂度导致的执行难度。

一旦任务拆解完成，云端将这些子任务分配给端侧的小模型进行执行。每个小模型负责执行特定的任务，如物体抓取、避障等。这些小模型通过内置的计算机视觉和传感器系统，能够实时感知环境中的变化，识别物体的位置，并根据云端提供的任务指令进行精准操作。例如，当小模型需要抓取桌上的杯子时，它会通过视觉系统定位杯子的位置，并通过控制系统确保抓取过程顺利进行。

在执行过程中，端侧的小模型会实时采集反馈信息，并将这些数据发送回云端。这一反馈机制是系统自我优化的重要部分。云端根据反馈信息对任务执行进行评估和调整，优化任务拆解或路径规划。通过这种方式，系统能够不断根据环境变化调整策略，提升执行效果。云端还可以通过分析反馈数据来调整未来的任务拆解策略，使得系统在执行过程中变得更加智能化和灵活。

最终，经过一系列的反馈和优化后，任务会顺利完成。系统通过持续的优化和调整，确保每一次任务的执行都尽可能达到预期目标。在任务执行的过程中，系统能够根据实际环境的变化动态调整策略，从而为未来任务的执行提供智能化支持，确保系统的长期高效运行。

5 实验设计与验证方式

5.1 环境与平台

为了全面评估本系统在任务泛化、多智能体协同与隐私保护等方面的性能表现，本文选择使用 AI2THOR 平台作为主要的实验环境。AI2THOR 是一个基于虚拟现实的三维环境仿真平台，广泛应用于计算机视觉、强化学习与机器人行为建模等领域，具备高可定制性和真实物理交互建模能力。其丰富的场景类型（如厨房、客厅、办公室等）与细致的对象属性设置，为本项目提供了一个高度仿真的测试环境。

通过 AI2THOR，研究者可以灵活定义实验环境的多项参数，包括目标物体的位置、障碍物的布局、环境动态性等，从而构建不同复杂程度的任务场景。例如，在一个典型的家庭模拟环境中，系统可被要求控制多个机械臂协同完成“从餐桌上抓取杯子并放置到货架上”的任务，过程中需避开诸如盘子、餐具等障碍物。这种设置可有效验证系统在多物体干扰、动态布局与自然语言指令解析下的综合处理能力。

针对本项目“多机械臂协同执行”的核心设计，我们进一步构建了异构多臂实验场景，即模拟多个具备不同操作能力、视觉范围或动作精度的机械臂，同时完成一个复杂任务的分工协作。在该实验中，不同机械臂将被分配不同的子任务（如识别物体、执行抓取、完成搬运、主动避障等），并需实时与其他智能体进行信息交换与动作协调，以完成整体任务目标。此设置重点考察系统在任务拆解、资源调度与冲突规避方面的智能调控能力。

此外，为了验证联邦学习模块的有效性，我们将在不同端侧模拟多个数据偏好的子模型（如在视觉分布、操作风格、任务偏好上存在差异），测试系统在不共享原始数据的前提下，如何通过参数聚合与知识蒸馏实现能力迁移与性能提升。

通过以上设置，实验将从任务完成率、执行效率、协同稳定性、任务泛化能力以及端侧隐私保护等维度对系统进行综合评估，为后续系统优化与实际部署提供依据。

5.2 验证指标

为了全面评估系统在多任务、多智能体协同执行中的综合性能，本项目设计了四类关键性指标，从准确性、适应性、隐私性与实时性等维度验证系统的有效性和实用价值。

1. 执行成功率

执行成功率是衡量系统完成任务准确性与稳定性的核心指标。在实验过程中，系统将对每次任务尝试进行记录，并根据任务是否达成预期目标进行判定。成功标准包括：机械臂是否按

指令完成动作流程，是否准确避障，以及目标物体是否被正确放置于指定位置。通过对不同任务与场景下的成功率统计，可定量评估系统的鲁棒性和执行可靠性。

2. 任务泛化能力

任务泛化能力反映系统在未见过的新任务、新环境条件下的适应性，是评估智能系统“学习–迁移–应用”能力的重要指标。我们将在实验中设置多种类型的物体、不同任务目标及多样化的场景布局，以测试系统在“零样本”或“迁移”条件下的表现。系统能否在不依赖额外训练的情况下灵活应对复杂变化，将直接体现其智能水平与应用潜力。

3. 隐私保持能力

隐私保护是本系统架构中的核心特征。借助联邦学习机制，系统实现了在不上传原始数据的前提下进行本地模型训练与全局知识聚合。隐私评估将从以下两方面展开：一是验证本地数据是否在训练过程中完全保留在端侧；二是检验系统在使用参数聚合、模型蒸馏、加密传输等机制后，是否能够有效避免用户敏感信息泄露。同时，我们也将对比传统集中式训练方式下的隐私风险，突出联邦机制的优势。

4. 系统响应时延

系统响应时延是指从接收到用户指令到机械臂实际开始动作之间的延迟时间。该指标直接关系到多机械臂系统在动态环境中的实时性与任务协调能力。响应时延较高可能导致智能体间调度混乱，影响整体协作效率。实验将记录各阶段响应时长，并分析在不同负载、通信策略下的系统反应能力，评估系统对时间敏感任务的适配性能。

通过执行成功率、任务泛化能力、隐私保持情况与系统响应时延四大维度的综合评价，我们将从准确性、智能性、安全性与时效性等方面全面衡量系统性能。实验结果不仅为后续系统优化与模块迭代提供理论支持，也为其在实际场景中的部署与推广提供重要参考依据。

5.3 实验结果与分析

为验证系统在不同环境中的实际表现，我们在 AI2THOR 平台上构建了 4 种典型任务场景（如家庭厨房、办公桌面、仓储架台、走廊避障），并部署 4 台异构机械臂代理分别进行协同任务测试。以下为关键实验结果：

表 1 多智能体系统仿真测试结果表

指标类别	具体含义	4 场景均值	标准差
执行成功率（%）	完成任务次数/总任务次数	92.4	±3.2

任务泛化成功率（%）	在未训练场景下成功完成任务的比率	86.7	±4.1
响应时延（秒）	指令下发至执行启动的平均时间	0.83s	±0.12
数据上传量（KB）	每轮联邦学习平均上传参数量	<150 KB	—
隐私泄露检测率（%）	联邦过程中是否可推测原始数据（逆推攻击测试）	<1%（近于0）	—

6 应用场景与推广潜力

6.1 典型场景应用

本项目研发的多智能体机械臂协作系统，具备任务理解与自主执行能力、支持多设备协同与跨场景泛化，在多个典型应用领域中均展现出广泛的应用潜力与现实价值。以下列举三个具有代表性的场景，以展示其在工业、服务与医疗等行业中的多样化应用前景。

（1）智能仓储物流系统

在电商、快递、第三方仓储等行业的推动下，现代物流系统对自动化程度提出了更高要求。当前仓储场景面临作业密集、人力成本高、订单响应速度要求快等问题，亟需更灵活高效的智能解决方案。本项目提出的多智能体机械臂协作系统，能够构建由多个端侧机械臂组成的“柔性作业网络”，每个机械臂根据云端下发的任务计划，独立而协同地完成搬运、分拣、装载、上下架等子任务。

与传统 AGV 与固定路径系统不同，本系统可在**动态任务与障碍变化环境下实时规划路径并协同执行**，显著提升仓库空间利用率与单位时间内的任务吞吐量。同时，依托于联邦学习架构，系统可在不采集原始数据的前提下，根据不同仓储环境（如冷链仓、超高货架仓、跨楼层立体仓）优化模型策略，实现场景自适应与精度提升，从而增强系统对复杂环境的泛化与持续优化能力。

（2）家庭与养老服务机器人

随着老龄化社会加速到来，传统依赖人力的家庭照护模式正面临成本高、供给不足、服务质量不均等问题，服务机器人正成为智能助老的重要方向。本项目中的多智能体系统可嵌入服务机器人形态，协助老年人完成生活起居、物品搬运、环境清洁、健康提醒等任务。

例如，面对“帮老人从餐桌上拿水杯”的任务，系统可由大模型智能解析意图，判断“水杯”与“就近路径”，再将任务拆解为“移动至桌旁”、“避开桌椅障碍”、“抓取杯子”等子动作，由机械臂在狭小空间内灵活完成操作。同时，借助联邦学习机制，系统可通过不同家庭环境下的长期交互数据，优化任务策略，形成“因人而异”的服务模型，并确保用户隐私不被上传或泄露，实现真正的“个性化安全助老服务”。

（3）医疗辅助协作臂

在医疗场景中，尤其是在外科手术、精准定位、器械辅助等任务中，机器人协作系统对精度、稳定性、响应速度的要求极高。传统单臂手术机器人虽然已具备一定自动化能力，但在多部位配合、医生协同需求强烈的复杂手术中，仍存在效率瓶颈和动作冲突问题。

本项目系统基于**端云协同的任务理解与路径规划机制**，可实现多个机械臂间的同步执行、避障规划与手术节奏协调。例如，在神经外科手术中，主机械臂负责器械递送，辅机械臂负责吸引/支撑，系统根据医生语音或指令生成计划路径，实时判断最优交互策略，提升操作精度和人机协作效率。同时，通过术中操作反馈与联邦学习机制的持续积累，系统可提升对特定病种、术式的适应能力与成功率，为高精度医疗机器人提供可扩展的智能支撑。

6.2 拓展性说明

本项目在系统架构设计之初即充分考虑了未来技术演进和多场景部署的需求，强调模块化、可插拔、任务无关、模型可变等关键特性，从而具备高度的拓展性与适应性。无论是设备规模的扩大、任务复杂度的提升，还是运行环境的异构化，系统均能够通过灵活组合和动态调整，满足实际应用的多样化要求。

（1）支持设备规模扩展：多机械臂系统的水平可扩展性

系统采用去中心化的协同架构，允许在不修改核心控制逻辑的前提下，平滑接入更多机械臂终端，极大增强了部署的灵活性与系统的可扩容能力。随着任务负载的提升或作业范围的扩展，用户可以根据需求动态添加机械臂数量。得益于任务调度模块中的分布式任务分配与冲突规避算法，即使在大规模多臂同时工作的情境下，系统也能通过动态任务切分、空间避让和协同路径规划等策略，实现高效有序的资源分配，避免执行过程中的冲突与重复操作。例如，在大型智能仓储中心或自动化流水线生产车间，部署 10 台以上机械臂同时作业，系统可根据作业优先级、臂长范围、负载能力等参数，实现任务精细调度与负载均衡，保障整体系统的高效运行。

（2）适应多样任务类型：泛任务执行能力

针对现实中机器人所面对的任务日趋复杂、类型不断扩展的趋势，本系统构建了面向任务无关性的统一任务表达框架。系统不局限于“物体抓取”这类传统任务，还支持清洁、检测、调试、交互等多种任务类型。通过云端大模型对自然语言指令或多模态输入的理解，可将任务抽象为一组具有逻辑结构的子任务流程，并下发至端侧小模型进行具体执行。端侧模型则依托任务执行库与路径生成机制，完成不同任务动作的组合执行。此外，系统还支持通过在线学习和联邦优化，不断“看到新任务，学会新技能”，逐步构建起涵盖不同语义目标与操作形式的任务迁移能力。例如，系统可在完成“从桌上拿水杯”后，快速适应“整理书架”或“递送遥控器”等语义类似却操作路径不同的任务，展现出较强的跨任务泛化能力。

（3）兼容多类模型部署：云-端异构适配能力

本系统特别强调模型与算力环境解耦的能力，具备高度的模型通用性与跨平台运行能力。对于云端部分，可部署大规模语言-视觉-动作融合模型（Qwen2.5-VL-32B-Instruct），用于高层语义理解、复杂任务规划与全局决策。而端侧则根据设备的实际算力、能耗限制和响应速度需求，部署轻量级 Transformer 或卷积控制模型，专注于本地视觉识别与动作执行。通过统一的接口协议和模型调度机制，系统可灵活切换模型类型与大小，实现“任务难度-模型能力-设备算力”的动态匹配。例如，在工业车间内配置 GPU 节点的机械臂可使用中型模型执行精细任务，而家用服务机器人则可在 ARM 平台上部署极简模型，实现低功耗、响应快的日常任务服务。这种“云强端稳”的协同机制，不仅保证了系统性能与响应速度的平衡，也为后续模型升级、替换与迁移提供了良好的扩展接口。

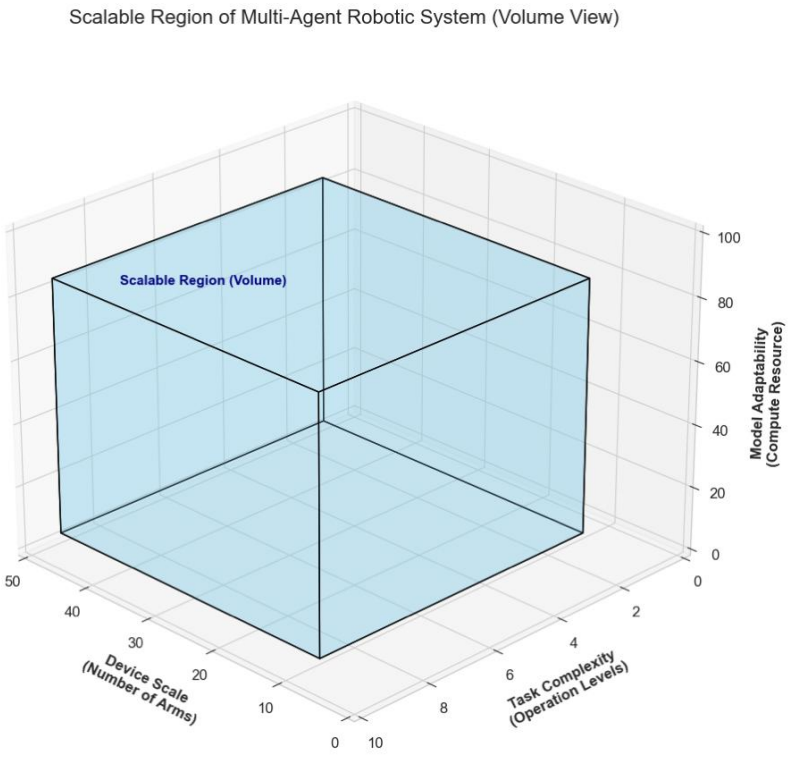

图 2 系统拓展性三维能力示意图，表示：在给定的设备规模（X 轴）、任务复杂度（Y 轴）和模型/计算资源适应性（Z 轴）这三维条件下，系统可以部署并保持有效运行的可能区域

7 创新点总结

本项目围绕多智能体协作、端云协同架构与联邦学习机制，提出了一种兼具任务泛化能力、隐私保护与高效执行能力的智能机械臂系统。系统创新性地融合了大模型智能体的全局规划能力与端侧执行器的局部感知能力，并通过联邦学习实现跨设备知识共享。以下为本项目的四个核心创新点：

1.首创性地融合大模型 Agent 与联邦学习的多执行体架构

本项目创新性地将大语言模型（Qwen2.5）作为云端智能体（Agent），与端侧的小模型执行器通过端云协同架构实现联动。这一结构突破了传统单体控制的限制，实现了“认知-拆解-执行”任务流的解耦式处理，大模型负责复杂任务的语义解析与策略规划，小模型专注于动作执行与反馈响应，从而显著提升了系统的整体智能水平与资源调度效率。

2.支持任务拆解与动态执行的协同机制

系统引入动态任务分解与实时策略调整机制，能够根据指令复杂度与环境变化，将任务自动拆解为多阶段可执行子任务，并由多个执行体并行协作完成。该机制不仅增强了系统在多任务场景下的适应能力，还提升了执行精度与响应速度，尤其在多物体、多障碍环境中展现出良好的泛化表现。

3.联邦知识蒸馏实现隐私保护与模型个性化兼容

为解决数据隐私与模型共享之间的矛盾，本项目引入联邦学习框架，通过在各端侧本地完成模型训练并采用知识蒸馏方式进行模型融合，有效实现了知识迁移与个体模型的个性化优化。该机制不仅保证了用户数据不出本地，还显著提升了系统在不同任务偏好与终端能力差异下的稳健性与普适性，真正做到了“协同共享，个性执行”。

4.基于 AI2THOR 平台完成多任务、多设备仿真验证

项目在虚拟仿生环境 AI2THOR 中进行了多轮测试，验证了系统在多任务、多终端协作条件下的泛化能力与执行效率。实验显示，本系统在面对复杂、动态的仿真环境时，能够灵活规避障碍、合理分配资源、协同完成任务，展现出良好的稳定性与鲁棒性，为后续实物部署与真实场景应用提供了有力支撑。

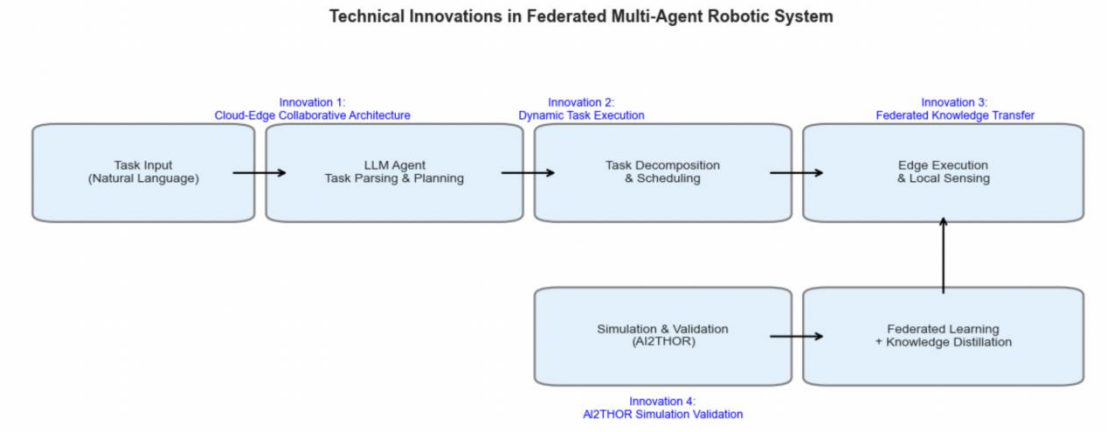

图 3 本项目所提出的联邦多智能体机械臂系统的技术创新框架图。
系统通过融合端云协同结构、动态任务拆解机制、联邦知识蒸馏方法以及基于 AI2THOR 的仿真验证，实现了任务泛化能力、执行效率与隐私保护的统一，展现出在多任务、多设备协作场景下的高度适应性与可扩展性。

本项目不仅在技术架构上融合了多项前沿人工智能方法，更在任务适应性、系统协同效率与隐私保护能力方面取得了显著突破。其模块化、可扩展、高适应性的设计理念为未来智能机器人系统提供了可复制的范式。随着技术生态的进一步成熟，项目具备广泛的落地潜力，可推广应用于智能制造、智慧物流、家庭服务、医疗辅助等多个关键行业，为智能机器人领域的发展注入新的动能。