ICS 35.240
CCS L70

团 体 标 准

JH/CAA 004-2024

联邦智能 通用技术框架

Federal Intelligence General Technical Framework

（征求意见稿）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上

2024-xx-xx 发布　　202X-xx-xx 实施

中国自动化学会　发 布

目　次

前　言

本文件按照GB/T 1.1-2020《标准化工作导则第1部分：标准化文件的结构和起草规则》的规定起草。

本文件由中国自动化学会联邦数据与联邦智能专业委员会提出。

本文件由中国自动化学会归口。

本文件起草单位：

本文件主要起草人：

引　言

联邦智能指在分布式的联邦数据间，以联邦控制、联邦认知、联邦计算、联邦安全为核心的面向隐私保护和数据安全、资源系统管理的统一整体，从而实现服务联邦化。基于单点的数据开发难以发挥大数据的优势和满足多场景的需求，联邦智能为解决大规模数据要素流通和治理场景下多源数据的感知、控制、协同、计算和保护等问题提供了一种切实有效的解决方案，致力于打破数据“孤岛”。联邦智能基于人工智能和大数据技术实现群体智能，驱动整个生态的创新和发展。

本文件可为联邦智能提供基础参考，有助于理解什么是联邦智能，有助于参与联邦智能各个环节和角色的各相关方开展数据开发利用和智能服务。此外，本文件有助于在保护数据隐私的前提下多方协作开展数据开发利用，有助于打通数据生产到使用再到服务与智能的环节，对于促进数据要素流通具有重要意义。

联邦智能 通用技术框架

1 范围

本文件规定联邦智能通用技术框架的组成，包括联邦数据、联邦控制、联邦认知、联邦计算、联邦安全和联邦服务六部分。

本文件适用于指导面向大规模数据共享和安全流通指导性技术框架设计规划，以及涉及多领域跨节点协作、数据隐私保护、多智能体系统等应用场景的设计与实现。

注：应用场景可包括需要分布式计算、协同智能处理以及隐私保护的复杂场景等。

2 术语和定义

下列术语和定义适用于本文件。

2.1

联邦节点 federation node

接受控制和管理的基本单元，一般存储节点目标、节点模型、节点数据、节点状态等，并具有数据控制权。

2.2

联邦数据 federal data

由独立实体拥有和管理，同时可以被其他实体在本地使用的数据。

2.3

联邦控制 federal control

采用分布式控制架构对联邦节点进行彼此独立的控制和管理。

2.4

联邦认知 federal cognition

利用认知智能技术，在联邦数据环境中进行认知分析及决策。

2.5

联邦计算 federal computation

协同联邦节点数据，完成模型训练或推理的计算过程。

2.6

联邦安全 federal security

在联邦计算过程中保护数据安全、计算安全、模型安全等的技术措施。

2.7

联邦服务 federal services

通过注册与调用、智能服务编排、场景化应用定制等对外赋能。

2.8

联邦智能 federal intelligence

一种基于独立自治而又相互协同的联邦节点实现智能的方法。

3 概述

联邦智能通用技术框架以“原始数据不出域、数据可用不可见”模式为核心，通过搭建基于联邦节点的联邦智能通用技术框架，以分布式的节点数据作为基础，通过联邦节点和联邦控制实现数据联邦化，进而利用认知智能技术在分布式数据环境中学习和计算，形成面向隐私保护、数据安全和资源协同管理的统一整体，支持跨组织、跨区域的数据安全共享和价值流通，实现联邦智能。

4　总体要求

4.1 联邦智能应具备不少于3个联邦节点，每个联邦节点经过认证，并保留数据控制权。
4.2 联邦智能的节点数据只能联邦成员可以使用。
4.3 联邦智能应支持数据安全的共享和使用。
4.4 联邦智能应持续对模型的传输和数据的使用进行监控，并记录。
4.5 联邦智能节点应接受联邦控制中心的管理和调度。
4.6 联邦智能应支持感知智能和认知智能。
4.7 联邦智能的节点应具备计算支撑能力。
4.8 联邦智能在运行过程中，当节点不满足使用要求时，应采取合理的控制策略。
4.9 联邦智能应不存在由于功能异常表现导致的数据安全等方面的不合理风险。

5　联邦智能总体框架

5.1　框架组成

联邦智能通用技术框架由联邦节点、联邦控制、联邦认知、联邦计算和联邦安全组成。

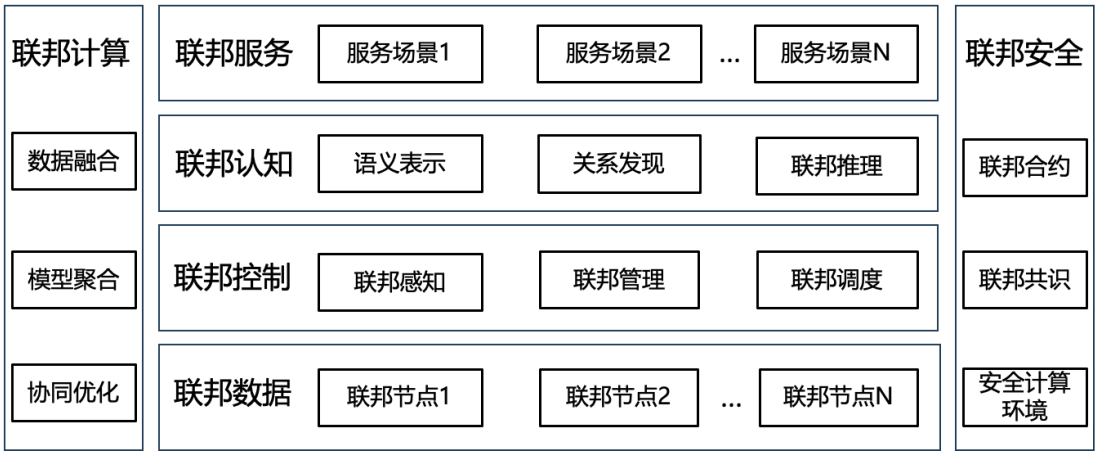

图 1　联邦智能通用技术框架

5.2　联邦数据

5.2.1　一般要求

由一系列联邦节点构成，并通过节点数据进行信息交流和协作的分布式网络。一般包含隐私联邦数据和非隐私联邦数据。

5.2.2 隐私联邦数据

隐私联邦数据不离开本地，仅限本节点使用，包括参数、状态、数学模式、结构、设置等隐私信息。

5.2.3 非隐私联邦数据

非隐私联邦数据实行所有权和使用权两权分离机制。

a) 数据所有权归本地节点所有，使用权由本地节点转移到联邦控制中心。

b) 通过加密算法进行上传和使用。

5.3 联邦控制

5.3.1 一般要求

联邦控制是基于分布式协同控制，实现多联邦节点的联合控制建模。应具备联邦感知、联邦管理、联邦调度能力。

5.3.2 联邦感知

联邦感知是多个联邦节点共同参与感知任务，每个节点在本地处理其所感知的数据，汇总部分结果用于全局任务。

a) 感知对象为联邦数据。

b) 联邦节点间共享必要的模型参数或感知结果，而不传输原始数据。

5.3.3 联邦管理

联邦节点的元数据管理，规定联邦节点的注册、选择策略和节点的协作方式等。

a) 联邦节点元数据包括定义、抽取、命名和版本管理等。

b) 联邦节点注册到控制中心，注册内容包括节点名称、版本、标签、环境、网络位置等信息。

c) 根据任务的安全等级、分析模式等选择节点。

5.3.4 联邦调度

对于联邦节点具有灵活的准入与准出机制，实现联邦节点的访问、过程监控等。

a) 联邦节点通过验证，接入到联邦智能系统网络中。

b) 允许联邦节点经联邦控制中心批准后获得准出资格。

c) 根据节点状态、节点数据情况等选择节点，并对节点开启接入、更新、停止等控制。

5.4 联邦认知

5.4.1 一般要求

联邦认知是在分布式数据环境中，共享和整合认知能力，实现更加智能化和协同的智能决策能力。

5.4.2 语义表示

整合多个联邦节点的语义信息，包括语义理解、知识表示、信息检索、自然语言生成等。

5.4.3 关系发现

跨节点的发现信息之间的关系，包括层次关系、依赖关系、连接关系等。

5.4.4 联邦推理

从联邦节点中实时获取和更新信息，并对其进行关联和整合，通过不断演化，实现认知智能。

5.5 联邦计算

5.5.1 一般要求

联邦计算是通过在联邦节点本地设备上进行模型训练或推理，并在不共享原始数据的情况下进行模型参数更新和聚合，从而允许多个联邦节点协作完成任务。其中，数据融合用于各节点间的特征整合，模型聚合用于生成高质量的全局模型，协同优化确保整个计算过程中的高效性和可持续性。

5.5.2 数据融合

对多个联邦节点上的数据或特征进行融合，通过特征或模型的训练推理结果进行整合，促进模型的集体优化，并减轻数据孤岛问题。融合方法包括但不限于排序融合、级联融合、贝叶斯融合等。

5.5.3 模型聚合

每个联邦节点完成本地模型训练后，将本地设备上的模型参数或更新结果上传到联邦控制中心，并对这些模型进行聚合，生成全局模型。常见的聚合方法是加权平均，每个节点根据其数据量或质量贡献不同权重。

5.5.4 协同优化

优化分布式环境中节点之间的同步与信息传输，解决联邦节点与服务器之间的协同问题，尤其是在通信资源有限的情况下，确保整个计算过程的高效性和可持续性。协同优化方法包括但不限于减少参数传输频率、压缩模型参数、量化等。

5.6 联邦安全

5.6.1 一般要求

联邦安全是利用区块链、隐私保护等安全技术，建立联邦合约、联邦共识、安全计算环境等安全机制，实现计算过程中的数据安全和模型安全。

5.6.2 联邦合约

联邦合约具有自我验证、去中心化、可编程、不可篡改等特点。具有访问控制、非隐私联邦数据交换、局部状态修改、全局数据更新、意外情况处置等功能。

5.6.3 联邦共识

在去中心化系统中各联邦节点就记账权归属达成一致协议。

在有中心化系统中，中心节点对边缘节点的行为进行统一协调。

5.6.4 安全计算环境

在去中心化系统中各联邦节点提供联邦计算的安全策略、安全协议、安全规则，包括身份可信、数据可信、访问控制、安全审计、可信验证、数据隐私保护、模型参数保护等功能。

5.7 联邦服务

联邦服务是多个联邦节点基于联邦激励协作提供统一的功能或服务，每个服务或节点可以独立运行并处理本地数据，它们共同协作形成一个整体的服务生态系统，可服务的场景包括但不限于金融、医疗、政务等。