1. 该申请项目是否面向国家需求并试图解决技术瓶颈背后的基础问题？请结合应用需求详细阐述判断理由。

数据安全与国家安全和经济社会发展息息相关，因此数据隐私保护技术一直以来都是国家非常重视的技术之一。针对数据隐私保护技术的研究很多，大部分都是针对单区域或者单领域场景，存在就比较严重的数据和服务的“孤岛现象”。本项目针对当前人机物融合群智计算架构落地应用中存在的“群体智能与数据隐私保护融合”和“多源异构数据交互共享中数据隐私保护”两个关键科学问题，拟以区块链和机器学习融合技术为核心，研究面向服务分级分类的只能可信区块链构造技术、面向数据隐私和服务区块链的可信用户和聚合中心智能评估和选取技术以及只能可信数据聚合技术。最终完善数据汇聚全过程的数据隐私保护体系，为未来发展人工智能的广泛应用提供数据隐私保护理论基础和技术支撑。

1. 请评述申请项目所提出的科学问题与预期成果的科学价值。

针对人机物融合智能计算架构数据汇聚过程中的数据隐私保护受到服务“孤岛”和数据“孤岛”制约的现状，本项目集中研究“群体智能与数据隐私保护融合”和“多源异构数据交互共享中数据隐私保护”两个关键科学问题。前者是考虑人机物融合智能计算数据过程中的数据隐私威胁的特征，对于数据隐私保护有了智能化的需求。因此，通过群体智能提高汇聚数据的隐私性，通过汇聚数据的隐保护来确保群体智能的高效、可靠、可控成为亟需解决的问题。后者则是考虑当前人机物融合群智计算多源异构数据汇聚过程中面临着数据跨区域、跨领域、跨链互操作难和和多元异构数据交互共享时的隐私安全问题。本项目着重研发面向服务分级分类的只能可信区块链构造技术、面向数据隐私和服务区块链的可信用户和聚合中心只能评估和选取技术以及智能可信数据聚合技术。最终突破跨区域、跨领域数据汇聚过程中服务数据分割、互操作性缺失、隐私保护难的瓶颈；突破跨区域、跨领域数据汇聚过程中用户和聚合中心的隐私泄露行为监管困难的瓶颈；突破现有数据聚合技术无法实现隐私保护和聚合精度平衡的瓶颈。这些预期成果对于人机物融合智能计算的应用具有重要的科学价值，能够为广泛的人工智能领域的落地应用的数据隐私安全提供理论基础和技术支撑。拟解决的科学问题很重要，

1. 请评述申请人的研究基础及研究方案的创新性和可行性。

申请人长期从事数据安全、隐私保护、网络安全优化方面的理论和应用研究，在网络与信息安全方面具有很好的研究基础，对于隐私保护技术、信任管理模型和及其学习模型等研究方案比较熟悉，且具有较强的仿真实验和系统开发经验。申请人已经对人机物融合群智计算中数据数据隐私保护做了比较全面的预研，提出的研究方案具有较好的创新性：1）提出基于跨区域同构、跨领域异构、跨区域与领域同异构终极连结构的智能可信区块链；2）提出基于内外中继链构造的用户、聚合中心信用存储机制，保障选取用户和聚合中心的安全可靠；3）设计基于差分隐私噪音扰动的隐私保护机制，提出基于深度强化学习的数据真实性检验技术，最终提出隐私保护与聚合精度平衡的数据聚合技术。同时，作者对于模型的构建、研究方案的设计、关键技术的解决以及实验方法都给出了清晰的技术路线，其中有些关键技术已经应用于工业物联网中且已经取得不错的成果。因此，整体研究方案是可行的。课题组中有若干研究人员和博士生，能够胜任该课题的研究任务。

1. 其他建议