

《端侧多模型资源隔离与调度安全要求》标准编制说明

标准编制组

1. 标准范围

本文件规定了智能终端设备（包括但不限于智能手机、车载终端、物联网终端等）上同时部署运行多个人工智能模型在资源隔离与调度方面的安全技术要求。

本文件适用于智能终端设备上多模型的部署、运行与调度场景，可为端侧模型服务提供者的设计、开发、部署和运维活动提供参考，也适用于第三方评估机构等组织进行安全评估。

2. 工作简况

3. 标准编制原则和确定标准主要内容

本标准规定终端设备上同时部署运行多个人工智能模型在资源隔离与调度方面的安全技术要求。适用于智能终端设备上多模型的部署、运行与调度场景，可为端侧模型服务提供者的设计、开发、部署和运维活动，也适用于第三方评估机构等组织进行安全评估。

本标准核心内容包括：规定端侧多模型的计算、存储、数据、权限四类资源隔离，要求独立沙箱、加密存储、数据清理与最小权限；调度上建立安全等级优先级，防资源独占，支持并发控制、异常熔断与加密审计日志等。

4. 主要试验(或验证)的分析、综述报告

无。

5. 标准在起草过程中遇到的问题及解决办法；重大分歧意见的处理经过和依据；有无重要技术问题需要说明

在本文件的修订过程中，无重大分歧意见和技术问题。

6. 与国外标准的关系：包括：采用国际标准和国外先进标准的程度，与国外标准主要技术内容的差异

该项目没有对应的国际标准或国外先进标准。

7. 修订标准时，说明与标准前一版本的重大技术变化，并列所涉涉及的新、旧版本的有关章条(可引用标准前言的内容)；废止/代替现行有关标准的建议

不涉及。

8. 说明标准与其他标准或文件的关系(可引用标准前言的内容)，特别是与有关的现行法律、法规和强制性国家标准的关系

符合现行法律、法规要求。

9. 标准作为强制性标准或推荐性标准的建议

建议本文件作为推荐性标准。

10. 贯彻国家标准的要求和措施建议(包括组织措施、技术措施、过渡办法等内容)；标准发布后，对国内外业界可能产生的影响

建议本文件作为推荐性标准发布实施。

本文件旨在规范终端设备上同时运行多个人工智能模型时的资源隔离与调度安全技术要求，确保多模型环境下的数据安全、模型安全、系统稳定性和资源公平性。

随着端侧AI应用日益普及，单个终端设备上可能同时运行多个AI模型（如语音识别、图像处理、推荐系统等）。不同模型在计算、存储、数据、权限等方面的资源需求和安全等级各异，若缺乏有效的隔离与调度机制，可能导致数据泄露、资源争用、模型干扰等安全风险。因此，制定统一的安全标准对于保障端侧多模型系统的安全性、稳定性和可审计性具有重要意义。

11. 标准是否涉及知识产权的情况说明；如标准中含有自主知识产权，说明产品研发程度、产业化基础及进程

本文件未涉及。

12. 其他应予说明的事项

本文件未涉及。