附件 1

2026 年山东省“人工智能+网络安全”揭榜挂帅榜单目录

序号	类别	项目名称	拟解决问题	成果形式
1	理论研究类	多元异构环境下安全资产智能管理关键技术研究	研究多元异构数据融合与安全资产自动发现关键技术，分析复杂网络环境下资产动态识别与画像构建机理，构建智能管理关键技术模型，提高安全资产精准识别与动态管理能力。	研究报告
2	理论研究类	多源威胁情报智能分析处置关键技术研究	围绕多源威胁情报分析中的关键问题，研究人工智能在威胁信息融合、异常行为与威胁事件识别、告警关联压缩、攻击实体关系挖掘、攻击路径推演及响应优先级评估中的作用机理，提升威胁发现、风险研判与响应决策能力。	研究报告
3	理论研究类	漏洞与恶意软件主动防御关键技术研究	围绕漏洞与恶意软件威胁防御中的关键问题，研究人工智能在风险精准评估、未知漏洞与异常行为识别、利用及攻击路径分析、告警与处置优先级排序、误报甄别与自动阻断中的作用机理，实现智能化漏洞治理与恶意软件主动防御能力。	研究报告
4	理论研究类	敏感数据智能识别管理关键技术研究	研究多源敏感数据动态识别与分类分级的关键技术机理，分析数据流转实时监控、异常行为研判及智能管理的核心问题，明确全流程防护与智能预警机制的实现路径。	研究报告
5	理论研究类	面向人工智能隐私保护计算的密码技术	研究面向人工智能隐私保护计算的同态加密与安全多方计算关键技术，剖析现有密码技术在人工智能任务中的关键瓶颈及其成因，构造适配卷积神经网络及大语言模型推理的安全计算方案，提升人工智能应用的安全性与计算效率。	研究报告

序号	类别	项目名称	拟解决问题	成果形式
6	理论研究类	人工智能应用安全风险治理机制研究	围绕人工智能应用中的安全风险与治理需求，系统研究算法偏差、数据污染、模型攻击、隐私泄露等风险类型及其形成机理，分析相关风险对社会治理、行业应用和网络安全的影响，探索风险识别、监测预警、分级治理、协同监管与防护机制，为政策制定、标准规范和安全治理体系建设提供支撑。	研究报告
7	实践探索类	安全资产高质量管理体系建设及应用路径探索	围绕安全资产全生命周期管理需求，梳理资产发现、业务关系与风险量化的核心问题，探索高质量管理体系建设的关键环节及智能化应用实施路径，提升安全资产管理的整体化与持续运行能力。	实践案例
8	实践探索类	人工智能驱动的网络安全态势感知关键技术研究	面向网络安全实战应用需求，研究人工智能在网络威胁信息分析、APT 攻击早期发现和态势感知中的应用方法，提升多源安全数据汇聚分析、异常行为识别、风险预警研判和运营支撑能力，探索可推广的应用模式、建设路径与协同机制，为网络安全防护能力提升提供实践支撑。	实践案例
9	实践探索类	人工智能驱动自动化渗透测试应用推广机制与行业适配策略研究	围绕自动化渗透测试实践需求，梳理人工智能在渗透流程化管控、漏洞自动化探测发现中的应用经验，探索主动防御能力建设与人工智能赋能自动化渗透测试的应用推广机制，明确针对各行业的具体适配策略。	实践案例
10	实践探索类	AI 赋能的边界自动防护体系应用示范与推广	围绕互联网边界防护漏防多的痛点需求，解决安全系统恶意访问检出率低，自动处置时效性差，安全防护不能多点联动等问题，探索边界防护的多系统情报 AI 分析共享，数据流实时阻断及多点联动防护的应用示范模式，提升边界防护能力，形成一个 AI 赋能的跨区域，自动防护系统。	实践案例

序号	类别	项目名称	拟解决问题	成果形式
11	实践探索类	人工智能驱动的数据安全治理与可信共享应用研究	面向数据开发利用及安全共享需求，研究人工智能在数据识别分类、流转监测、风险预警和安全管控中的应用方法，提升数据治理精细化水平和可信共享能力，探索跨场景应用模式、协同管理机制和实施路径，形成可复制可推广的实践方案，为数据安全治理与价值释放提供支撑。	实践案例
12	实践探索类	基于人工智能的全域安全运营防护体系研究及应用	围绕组织机构安全运营与全域网络防护需求，解决安全运营自动化水平低、态势感知滞后、决策辅助不足等问题，构建基于人工智能的全域智能安全网络体系，探索人机协同安全运营模式，突破多智能体协同与内生安全防护关键技术，全面提升安全处置效率与网络全域防御能力。	实践案例
13	实践探索类	供应链安全风险管理体系建设与应用探索	围绕供应链安全管理需求，梳理多维度风险评估、组件漏洞监控、事件溯源及风险预警的实践经验，探索基于人工智能的供应链安全管控体系建设及落地应用路径。	实践案例
14	实践探索类	人工智能全生命周期安全治理体系建设及应用研究	面向人工智能安全治理实践需求，研究覆盖数据、模型、应用等环节的安全治理方法，提升风险识别、监测预警、协同处置和综合管控能力，探索全生命周期安全治理的应用模式、实施路径和运行机制，形成可复制可推广的实践方案，为人工智能安全应用和规范发展提供支撑。	实践案例
15	实践探索类	人工智能赋能的工业互联网安全公共服务体系建设与应用	围绕工业互联网安全公共服务实践需求，梳理中小工业企业安全团队缺失、防护资源碎片化、告警误报率高、威胁研判依赖人工经验等突出问题，探索基于大模型与安全智能体的告警精准降噪、企业安全画像自动生成、攻击溯源智能研判、安全知识智能问答与自动化响应处置的应用路径，构建工业互联网安全公共服务体系，形成面向中小企业的轻量化安全服务模式，提升工业领域整体安全防护水平与政企协同治理效能。	实践案例

序号	类别	项目名称	拟解决问题	成果形式
16	实践探索类	互联网多模态敏感数据智能安全监管体系建设与应用探索	围绕互联网文本、图像、音视频等多模态复杂敏感数据识别监管需求，分析当前敏感数据识别、分析与处置关键环节实践基础，探索基于人工智能的互联网多模态敏感数据精准识别、流转监测与威胁研判等智能安全监管体系建设与应用示范，提升互联网数据安全治理智能化服务效能。	实践案例
17	实践探索类	人工智能系统网络安全保险服务模式创新与实践	针对人工智能系统在开发、训练、部署、运行各阶段面临的模型投毒、数据泄露、算法偏见、对抗攻击等新型网络安全风险，传统保险产品难以精准承保与定价。研发 AI 系统动态风险评估模型，设计与之匹配的网络安全保险产品及“技术加固+保险保障”服务套餐，并在数字政府、工业大模型等重点行业开展试点，形成可推广的 AI 系统安全风险金融对冲方案。	实践案例