2023 年 CCF-绿盟科技“鲲鹏”科研基金项目申报指南

一、总则

CCF-绿盟科技“鲲鹏”科研基金重点面向国内高校、科研机构的研究人员和团队，旨在以小微课题的方式支持科研人员的研究与创新，推动科研技术成果转化，促进外部科研机构优秀研发能力与公司内部产品价值的深度融合，构建互动合作与创新发展的生态圈，为绿盟科技的产品与解决方案创新赋能。

二、资助对象和条件

1.申请人须是国内高校、科研院所在职的全职教师或研究人员；

2.申请人须具有高级专业技术职务（职称）或具有博士学位，拥有一定数量的相关领域研究成果，能作为项目的实际负责人并担负实质性研究工作；

3.申请人同一研究项目只能申报一个同类科研基金，不能重复申报。

三、资助方式及项目范围

1.项目实施期为 1 年,单项资助额度原则上不低于 8 万元。

2.2023 年，CCF-绿盟科技“鲲鹏”科研基金重点资助的研究领域和方向：

（1）数据安全与隐私计算方向；

（2）人工智能赋能与对抗方向；

（3）新型网络安全攻防技术方向；

四、项目申请和评审

1.符合条件的研究人员在项目申报规定时间内填写《2023 年 CCF-绿盟科技“鲲鹏”科研基金项目申报表》并发送至 kunpeng2023@nsfocus.com，每位申请人仅限提交一份申请。

2.申请人在申报前需确认所在高校/科研院所可以作为项目依托单位签署科研合作协议，申请人本人可以作为项目负责人签署项目保密协议等相关承诺文件。任何针对项目申报的问题，请联系邮箱：kunpeng2023@nsfocus.com。

3.CCF 和绿盟科技成立联合项目组，共同邀请专家审核申请项目。专家评审时主要考虑：

（1）申请项目的研究意义，包括国内外研究现状以及市场前景；

（2）申请项目的技术基础，包括技术成熟度、自主知识产权积累、与主流技术对标或产品适配验证等情况；

（3）申请项目的主要研究内容，包括技术路线、研究内容、具体技术指标、创新性、支撑条件需求等；

（4）项目实施计划、预算设计的合理性；

（5）预期交付的成果形式及数量；

（6）申请者能力及团队保障条件，包括领军人物、团队学术水平和科研能力。

4.联合项目组依据专家审核意见，结合公司具体情况，确定资助的研究项目及资助强度等。

五、本期项目时间安排

项目指南发布	2023 年 9 月 1 日
项目申请截止	2023 年 10 月 8 日
答辩时间	2023 年 10 月 12 日-16 日
评审结果发布，签署协议立项	2023 年 10 月下旬
CNCC2023 典礼颁奖	2023 年 10 月 26 日
中期检查，提交报告	2024 年 4 月
项目结束，提交成果	2024 年 9 月
终期答辩	2024 年 10 月

项目进行过程中的具体时间节点，请关注 CCF-绿盟科技联合项目组通知。

六、项目经费管理

1.基金项目评审结果公布后的3个月内，CCF、绿盟科技、项目负责人及其所在单位四方需完成基金项目技术交底及项目合同书的签署工作，以确定各方责任和义务，鲲鹏基金支持的项目将依据项目合同进行管理。

2.合同履行期间，绿盟科技可根据需要委派领域专家（组）或其代表，对受资助人合同履行的情况进行检查、监督。CCF依据绿盟科技委托，根据确定的项目经费、项目执行检查情况及合同约定，将项目经费分阶段划拨至项目负责人所在单位。项目负责人按阶段提交研究成果和检查报告。

3.CCF-绿盟科技“鲲鹏”科研基金实行专款专用，该经费不得用于发放人员工资（可用于劳务费支出），可用于项目研发产生的相关设备费、材料费、试验加工费、信息资料费、差旅费、管理费等。

七、项目管理

1.项目立项后不可更换项目负责人。在项目研究工作中，如因项目负责人自身原因中断研究工作，而造成项目终止。项目负责人需根据项目合同书的经费使用说明，退回已拨经费。

2.绿盟科技按照合同条款约定定期检查评估全部资助项目，项目负责人需按照合同要求，按时填写提交《中期报告表》，并提交阶段成果。

3.项目完成后，项目负责人填写《结题报告表》，由联合项目组组织检查验收，项目负责人应将结题报告和合同中规定的相关技术成果完整提交给绿盟科技和项目负责人所在单位归档。

4.项目负责人原则上不可放弃基金资助，如有特殊情况，需提交《放弃基金声明》并加盖项目负责人所在单位公章后，由联合项目组存档留备。

八、成果管理

1.项目负责人在项目研究过程中形成的与项目相关的成果的著作权及专利等，包括但不限于论文、著作、源代码、研究报告和数据等，其知识产权权利归属项目负责人及其所在单位和绿盟科技三方共同所有。绿盟科技有权免费优先使用。使用的具体细节以与项目负责人和其所在单位签署的协议为准。

2.在此期间发表的论文及著作需标注“受CCF-绿盟科技‘鲲鹏’科研基金资助”字样。CCF有权将上述论文及著作收入CCF数字图书馆，供CCF会员阅读。

本指南自公布之日起实施。

CCF-绿盟科技“鲲鹏”科研基金项目组

2023年9月1日

2023 年 CCF-绿盟科技鲲鹏科研基金指南

1 数据安全与隐私计算方向

1.1 隐私计算关键问题研究

研究背景：

大数据、人工智能的广泛应用带来了数据隐私保护和模型安全的风险和挑战。面向大规模、分布式人工智能应用场景建模的实际需求，利用隐私计算技术，探索人工智能场景数据隐私标准格式，实现多场景多异构 AI 算法的高效融合、协同和框架验证。在运用隐私计算技术解决 AI 算法高效融合的同时，也需要注意隐私计算技术所带来的安全风险：例如投毒攻击、隐私窃取等。探索相关攻击与防御技术。

研究内容：

1.研究适用于联邦学习的半同态加密的隐私数据计算技术。

2.研究基于隐私数据计算技术的联邦学习大模型安全融合技术。

3.研究基于可信执行环境的人工智能模型隐私安全防护及验证框架，实现大模型技术的隐私保护、模型安全、联合建模等。

4.研究隐私计算相关安全风险与防御技术。

考核指标：

1.联合发表关于上述研究内容的高水平学术论文一篇（中国计算机学会推荐国际学术会议和期刊目录 B 类（以下简称 CCF-B）以上）。

2.联合申请至少一项发明专利。

3.输出技术报告 1 份。

4.基于主流隐私计算开源框架（FATE 或隐语）研制上述原型系统，要求以插件等形式与开源框架低耦合，可快速适配开源隐私计算框架的版本更新。要求无改动或改动较小的情况下，完成两个版本的适配，并提供源代码。其中指标要求包括：

（1）半同态加密。单台服务器条件下，基于 FPGA 或 GPU 加速，相较于 Intel i7 CPU 单核，至少需 10 倍计算加速效果。

（2）联邦学习大语言模型安全融合技术，要求适用：

a. LLM 参数规模至少 1 亿；

b. 广域网带宽条件（小于 100Mbps）。

（3）适配市场主流 GPU，实现 AI 大模型在可信执行环境中的硬件加速。

1.2 面向行业应用的数据安全防护系统

研究背景：

数据成为新型生产要素，需要在保护隐私的前提下，实现数据的安全采集、存储、使用、流转，为数据的开放与共享提供安全保障。特别是各类格式化和非格式化的数据在存储和流

转过程中的防护技术亟待研究。

研究内容：

1.研究基于同态加密、身份认证、可搜索加密、完整性审计等技术的数据安全技术方案，实现数据的安全存储、流转与密文计算。

2.研究主流数据库网络协议识别与防护技术。

考核指标：

1.联合发表关于上述研究内容的高水平学术论文一篇（CCF-B 以上）。

2.联合申请至少一项发明专利。

3.输出技术报告 1 份。

4.实现密文（有限）全同态计算的硬件加速功能，例如对 Microsoft SEAL 实现 FPGA 或 GPU 硬件加速，相较于 Intel i7 CPU 单核，至少需 30 倍计算加速效果，并提供源代码。

5.实现数据库协议解析原型系统一套，并提供源代码，其中指标要求包括：

数据库环境、解析文档、源代码等相关材料，其中系统支持解析数据库类型大于 30 种，版本类型大于 80 种，包括关系型、非关系型等数据库；上下行流量解析，支持语句、数据内容解析，压缩数据解析，支持关联查询、多层嵌套等常见复杂语句解析，解析准确率大于 95%；常见数据库客户端、应用系

统等连接，不同操作系统中的数据库部署方式等协议解析。

1.3 面向人工智能系统的全生命周期数据防护技术研究

研究背景：

数据已成为客户的核心资产，包括客户信息、商业机密、财务数据等。随着数据要素的流转和人工智能大模型的兴起，如何在合理使用数据产生价值的同时，有效保护客户数据安全不受侵害，同时支持将数据合理合法的应用于各类人工智能应用，相关数据安全技术应得到充分研究。

研究内容 ：

1.研究多维度安全的通用人工智能系统，实现数据跨域可控流转与融合利用，以及分散空间异构数据的融合、利用；

2.研究分散空间中的数据融合利用与隐私保护的需求，突破分布式联合训练技术；覆盖数据采集、模型训练、模型预测、模型溯源全生命周期的安全。

考核指标：

1.联合发表关于上述研究内容的高水平学术论文一篇（CCF-B 以上）。

2.联合申请至少一项发明专利。

3.输出技术报告 1 份。

4.研制面向通用智能系统的数据安全防护原型系统 1 套，支持文本、图像、音频、视频等多模态的数据，可抵抗多种攻

击，并提供源代码。

2 人工智能赋能与对抗方向

2.1 供应链网络精准画像和安全风险分析

研究背景：

随着全球供应链的不断发展和扩展，企业在获取原材料、生产产品和分销服务时,涉及的多个环节和参与方也逐渐增多。因此，针对供应链网络的结构、流程和参与者之间关系的画像和安全风险的研究变得必要。

研究内容 ：

研究供应链关键信息的自动化采集和网络构建技术，实现供应链网络的动态可视化。研究供应链网络安全风险分析、行业市场分析等工作，突破供应链安全隐患的早期感知难题。

考核指标：

1.联合发表关于上述研究内容的高水平学术论文一篇（CCF-B 以上）。

2.联合申请至少一项发明专利。

3.输出技术报告 1 份。

4.研制ICT供应链多源情报探测与图谱构建原型系统1套，并提供源代码，其中指标要求包括：

（1）系统采集的开源情报覆盖招投标平台、企业官网、龙

头企业公众号、企业公告、行业社群、行业分析报告、行业白皮书、国内外政府监管部门网站等多类型情报源200个以上；

（2）系统构建的产品链覆盖英特尔、AMD、路由器、交换机、网络接口卡、高性能计算机、服务器、大容量存储、防火墙、国产信创芯片、GPU、PCB、电源、光纤、基础软件、基站、屏幕、射频通信、天线、移动通信设备等对关键信息基础设施安全有重要影响的网络产品 20 种以上，产品构成的层级不少于3级的产品，实体链累计3万条以上。

（3)对于所采集的招投标网站等,至少完成98%以上的ICT相关采购数据的供应链信息抽取，抽取出的供应链信息准确率在95%以上。

2.2 图像视频深度伪造检测

研究背景：

随着图像和视频处理技术的进步和人工智能的应用，图像和视频的深度伪造技术变得越来越普遍和复杂，呈现出越来越高的仿真度和隐蔽性。因此，图像和视频的深度伪造检测的研究变得必要。

研究内容：

1.研究面向图像的深度伪造检测算法。基于深度学习技术，研究图像的深度伪造检测算法。检测算法的支撑技术包括但不

限于卷积神经网络（CNN）、长期循环卷积网络（LRCN）、生成对抗网络（GAN）等神经网络，以及各类特征提取和篡改定位等检测技术，提高对伪造图像的区分能力。

2.研究面向视频的深度伪造检测算法。针对视频深度伪造技术，全面捕捉视频伪造的特征，研究基于深度学习的视频帧级别和时序级别的检测方法。涉及的技术包括但不限于光流分析、迁移学习、胶囊网络、长短期记忆网络（LSTM）等。

考核指标：

1.联合发表关于上述研究内容的高水平学术论文一篇（CCF-B 以上）。

2.联合申请至少一项发明专利。

3.输出技术报告 1 份。

4.研制图像深度伪造检测原型系统 1 套，并提供源代码。

5.研制视频深度伪造检测原型系统 1 套，并提供源代码。

2.3 人工智能自身安全性研究

研究背景：

随着人工智能技术的普及，越来越多的系统和服务依赖于人工智能算法，包括金融、医疗、交通等领域的应用。然而，人工智能本身也面临着安全威胁，任何与人工智能相关的安全问题都可能对社会和经济产生重大影响。因此，研究人工智能

自身的安全技术，提高算法的鲁棒性、抵御攻击能力，对于已经广泛应用的人工智能系统而言是一个重要课题。

研究内容：

1.研究人工智能自身安全的攻击和防御机理。分析和研究数据、模型在训练和推理阶段面临的不同类型的攻击威胁，如对抗攻击、模型篡改等，并在此基础上，设计相应的恶意样本检测、算法鲁棒性评估等防御机制，增强人工智能算法的鲁棒性。

2.研究人工智能系统的隐私泄露风险和隐私保护技术。分析人工智能模型中的隐私泄露问题,如模型反演、模型窃取等；研究隐私保护的技术手段，包括差分隐私、同态加密等，确保在数据处理、模型训练和推理过程中用户和模型隐私安全。

3.研究模型可解释性。可从两个角度选择研究：一是研究人工智能模型的可解释性方法，解释模型的决策过程和关键因素，二是研究基于可解释性的人工智能攻防技术或攻防技术自身的可解释性。

4.研究人工智能模型的公平性问题。研究数据集中可能存在的各类偏见类型,以及针对不同偏见类型的公平性度量指标、纠偏技术。

考核指标：

1.联合发表关于上述研究内容的高水平学术论文一篇

（CCF-B 以上）。

2.联合申请至少一项发明专利。

3.输出技术报告 1 份。

4.研制 AI 模型鲁棒性增强技术验证原型系统 1 套，并提供源代码。

5.研制 AI 模型隐私性保障技术验证原型系统 1 套，并提供源代码。

6.提供人工智能模型可解释性相关技术 1 套，并提供源代码。

7 提供人工智能模型公平性度量指标或纠偏技术 1 套，并提供源代码。

2.4 基于对抗学习的攻击流量生成机制研究

研究背景：

随着近年来对生成对抗网络研究的增多，已出现了许多衍生模型架构，如何基于对抗学习生成攻击流量，确保其能够准确地模拟真实攻击，尤其是高度复杂的攻击行为，仍然是一个需要解决的问题。

研究内容：

1.研究基于对抗学习的攻击流量生成方法。

2.研究可解释的攻击流量生成方法，辅助分析人员理解模

型生成攻击流量的误差。

考核指标：

1.联合发表关于上述研究内容的高水平学术论文一篇（CCF-B 以上）。

2.联合申请至少一项发明专利。

3.输出技术报告 1 份。

4.完成基于对抗学习的攻击流量生成系统 1 套，并提供源代码，其中指标要求包括：

(1)变形后的攻击流量对入侵检测系统（IDS）的绕过率不低于 80%;

(2)攻击流量生成的种类和场景总数量不少于 50 个。

3 新型网络安全攻防技术方向

3.1 基于 GPT 大模型的新型欺骗式防御关键技术研究

研究背景：

随着未来数字城市的发展，万物互联、智能终端和网络用户数量的不断增加，关键信息基础设施面临着维护难度的增加和网络安全风险的加大。欺骗防御可以通过欺骗攻击者进攻虚假的攻击目标，从而分散攻击者注意力、延缓攻击，甚至提前发现攻击者的身份特征及攻击手段。而传统的欺骗防御通常需要大量的人工努力和时间来进行虚假系统服务、虚假信息资源

以及诱饵和欺骗漏洞的部署。基于 GPT 大模型的新式欺骗防御技术通过大语言模型生成符合上下文的操作响应，增强了欺骗响应的深度，大大减少了人工工作量，提高了防御效果。

研究内容：

针对当前欺骗防御深度浅、响应少的问题，研究一系列基于欺骗防御领域的大语言模型提示词，利用开源模型对话能力和逻辑推理能力，通过调整大语言模型的提示词，使其学会各种系统服务和信息资源的特征和响应，通过提示使其能够利用逻辑能力给出复杂情况下的虚假响应，以提升复杂情况下防御手段的欺骗能力，提高欺骗防御能力效果。

（1）研究漏洞防御方法和网络防御技术。

（2）研究基于欺骗防御技术的大语言模型技术。

考核指标：

1.联合发表关于上述研究内容的高水平学术论文一篇（CCF-B 以上）。

2.联合申请至少一项发明专利。

3.输出技术报告 1 份。

4.研制基于欺骗防御大语言模型的辅助响应插件，辅助防守方选择防守目标和手段，依据欺骗防御场景提供响应建议，并提供源代码。其中指标要求包括：

(1)支持 3 个常见的欺骗防御场景；

(2)构建一系列可应用于欺骗防御领域的大语言模型提示词。

3.2 容器编排系统第三方应用中冗余权限自动化检测及攻击展示

研究背景：

作为当前最流行的容器编排系统，Kubernetes 被广泛应用于各大公司和云计算厂商的云计算系统中。为了更好的管理集群和扩充功能，Kubernetes 在它的控制平面上运行了多个第三方应用。然而，这些第三方应用给整个集群的安全带来隐患。其中，第三方应用的权限滥用问题尤为突出，至今未得到系统化研究。

为此，本项目针对 Kubernetes 集群控制平面上第三方应用的权限滥用问题，自动化检测和识别应用的（过度）冗余权限，并演示如何利用这些冗余权限进行提权攻击。

研究内容：

1.研究容器编排系统第三方应用冗余权限的定义、自动化检测与识别。

2.研究容器编排系统第三方应冗余权限的利用及提权攻击展示。

考核指标：

1.联合发表关于上述研究内容的高水平学术论文一篇（CCF-B 以上）。

2.联合申请至少一项发明专利。

3.输出技术报告 1 份。

4.研制 Kubernetes 第三方应用冗余权限的自动化扫描和攻击展示工具 1 套，并提供源代码。

3.3 基于多主机攻击场景的威胁检测及攻击推理技术

研究背景：

随着网络环境的复杂化和攻击手法的多样化，单主机日志分析和传统的威胁检测方法难以对复杂的攻击进行有效的建模和分析。本课题旨在多主机场景下，通过溯源图构建技术还原攻击全貌；并利用图分析算法来有效地定位威胁事件，发现多种典型攻击；通过攻击推理技术有效地还原攻击者攻击意图与攻击过程。另一方面，由于多主机场景面临节点数量大的问题，如何将构建的溯源图进行高效的存储及清晰的可视化，也是当前亟待研究的一个问题。

研究内容：

1.基于主机日志或网络流量等多种数据，构建多主机溯源图。

2.基于多主机溯源图，实现攻击过程调查技术，溯源攻击

源所使用的网络设备，或主机进程/文件。；

3.研究基于多主机溯源图的攻击过程推理技术，实现多主机场景下的攻击路径还原。

4.构建网络攻击威胁子图模型，并基于多主机溯源图发现潜在的网络威胁。

5.溯源图存储及可视化技术。

考核指标：

1.联合发表关于上述研究内容的高水平学术论文一篇（CCF-B 以上）。

2.联合申请至少一项发明专利。

3.输出技术报告 1 份。

4.研制基于多主机攻击场景的威胁检测及攻击推理原型系统 1 套，并提供源代码。其中指标要求包括：

(1)能够分别基于主机日志或网路流量形成主机溯源图构建方法不少于 2 种，并能够准确形成包含多主机行为或事件的多主机溯源图；

(2)设计并实现可用的攻击调查方法/模型不少于 2 个，能够溯源得到攻击源，攻击源准确率达到 80%以上；

(3)设计并实现攻击推理方法/模型不少于 2 个，攻击路径还原测试准确率达到 80%以上；

(4)威胁子图模型可以匹配或适应不少于 10 种攻击场景，

并能够准确识别攻击类型，识别准确率达70%以上。