附件：

2025年度四川省科学技术奖拟提名项目公示信息（十二）

一、项目名称

面向数据全链路的联动防御关键技术及其应用

二、项目简介

当前，数据已成为驱动经济社会发展的关键生产要素，以数据为核心的新型产业模式正加速推动医疗、政务、金融、区块链等行业的深度变革。然而，伴随数据价值的持续释放，贯穿数据“采集—传输—共享—使用”全链路的安全挑战日益凸显。

在国家科技部、基金委等项目的支持下，项目组十年来联合攻关，针对采集数据难信任、传输数据难验证、跨域数据难共享、使用数据难审计等难题，重点突破了基于真值发现的数据可信采集、基于多层过滤的数据可验传输、基于联邦学习的跨域数据共享以及面向一体化审计的数据可靠使用等核心技术，形成贯通“采集—传输—共享—使用”的联动防御技术体系与产品，实现了四项创新：

1. 提出了基于本地差分隐私和轻量级同态签名的可信真值发现技术，实现了终端数据的机密获取与采集结果的可信验证，能够有效抵御数据篡改、结果伪造等攻击，并支持亚毫秒级别的数据采集和验证。

2. 提出了基于多层过滤检测与高效可验证的数据传输技术，在不可信云环境下同时保障传输数据的隐私性、规则匹配的机密性与传输过程的不可篡改性；具备 19GB 每秒的流量处理能力，通信开销降低十倍以上，支持 42 种协议流量解析。

3. 提出了基于相似度评估与自适应聚合的可验证联邦数据共享技术，在数据不出域的前提下，实现了大规模终端用户/设备数据的可信共享，对数据投毒、后门等攻击的检测成功率≥96%。

4. 提出了基于多模态检测与符号执行协同的数据审计技术，在保证使用数据可审计的前提下，支持漏洞语义建模、自动化执行与模糊测试，能够抵御单点失效等风险，覆盖 29309 种网络攻击检测规则。

项目组在 IEEE TIFS、IEEE TDSC 等高水平期刊和会议上发表论文 50 余篇，获国家发明专利授权 30 余件、软件著作权 5 项，制定国家和行业标准 6 部，相关成果得到 30 余位 ACM/IEEE Fellow 的引用和正面评价。

项目的实施使我国掌握了面向数据全链路的联动防御技术，形成了该领域产品的自主研发能力，项目成果已在浙江、山东、广东等 10 余个省份得到了成功应用，近三年产生直接经济效益 30.601 亿元，新增利税 3.111 亿元。项目成果还服务于成都世运会等国家重大活动，高质高效地完成了相关活

动的网络安全技术检测、24 小时实时监测、应急处置支持等工作任务，中共成都市委网络安全和信息化委员会办公室专门为此发来感谢信。

三、主要知识产权和标准规范等目录

知识产权（标准）类别	知识产权（标准）具体名称	国家（地区）	授权号（标准编号）	授权（标准发布）日期	证书编号（标准批准发布部门）	权利人（标准起草单位）	发明人（标准起草人）	发明专利（标准）有效状态
发明专利	在移动群智感知系统中实现高效隐私保护的真值发现方法	中国	ZL201811322088.3	2020 年 06 月 16 日	第 3844193 号	电子科技大学	李洪伟、刘森、徐国文、龚丽、任彦之、杨浩淼	有效
发明专利	云存储中可搜索加密审计日志的实现方法	中国	ZL201910602622.4	2021 年 07 月 09 日	证书号第 4535233 号	中国电子科技集团公司第三十研究所	汤殿华、李强、赵伟、熊维、黄云帆	有效
发明专利	在移动群智感知系统中可验证的、具有隐私意识的真值发现的方法	中国	ZL202010842682.6	2021 年 12 月 03 日	证书号第 4829078 号	电子科技大学	李洪伟、翟一晓、徐婕妤、郝猛、徐国文、刘鹏飞、杨浩淼、任彦之	有效
发明专利	在深度学习系统中基于数字指纹的验证与追踪方法	中国	ZL202011443755.0	2022 年 10 月 04 日	证书号第 5515478 号	电子科技大学	李洪伟、翟一晓、徐婕妤、徐国文	有效
发明专利	轻量级的密文相似度测试方法	中国	ZL202311712180.1	2025 年 08 月 08 日	证书号第 8142736 号	西华大学	曾晟珂、陈俊淞、王蒙、唐泽辉、周洁、熊玲、周恬恬、兰昔杰	有效
软著	亚信安全信舵统一安全扩展检测与响应平台 V6.0	中国	2025SR0347286	2025 年 02 月 27 日	证书号第 15003484 号	亚信科技（成都）有限公司	无	有效

软著	亚信联动防御系统 V6.0	中国	2025SR1330921	2025 年 07 月 22 日	证书号第 15987119 号	亚信科技（成都）有限公司	无	有效
软著	亚信安全管理与分析平台 V3.0	中国	2019SR0518208	2019 年 05 月 24 日	证书号第 3938965 号	亚信科技（成都）有限公司	无	有效
软著	非关系型数据库加密系统 V1.0	中国	2018SR488991	2018 年 06 月 27 日	证书号第 2818086 号	电子科技大学	无	有效
软著	基于 Spring-boot 项目的关系型数据库加密系统 V1.0	中国	2020SR0018452	2020 年 01 月 06 日	证书号第 4897148 号	电子科技大学	无	有效

四、论文专著目录

论文专著类别	论文专著具体名称	作者	发表日期	期刊/会议名称	类型
期刊论文	Privacy-preserving Efficient Verifiable Deep Packet Inspection for Cloud-assisted Middlebox	Hao Ren, Hongwei Li, Dongxiao Liu, Guowen Xu, Nan Cheng, Xuemin (Sherman) Shen	2022 年 06 月 22 日	IEEE Transactions on Cloud Computing (TCC)	中科院 JCR 一区
期刊论文	Privacy-Enhanced Federated Learning against Poisoning Adversaries	Xiaoyuan Liu, Hongwei Li, Guowen Xu, Zongqi Chen, Xiaoming Huang, Rongxing Lu	2021 年 01 月 01 日	IEEE Transactions on Information Forensics and Security (TIFS)	CCF-A
期刊论文	Deniable-Based Privacy-Preserving Authentication Against Location Leakage in Edge Computing	Shengke Zeng, Hongjie Zhang, Fei Hao, Hongwei Li	2021 年 12 月 27 日	IEEE Systems Journal	中科院 JCR 一区
会议	Catch You If You Deceive Me: Verifiable and Privacy-Aware Truth Discovery in Crowd Sensing Systems	Guowen Xu, Hongwei Li, Shengmin Xu, Hao Ren, Yinghui Zhang, Jianfei Sun, Robert H. Deng	2020 年 10 月 05 日	ACM ASIA Conference on Computer and Communications Security (ACM AsiaCCS)	安全领域著名会议

五、主要完成人

姓名	排名	技术职称	完成单位	工作单位
李洪伟	1	教授	电子科技大学	电子科技大学
徐国文	2	教授	电子科技大学	电子科技大学
吴永越	3	高级副总裁	亚信科技（成都）有限公司	亚信科技（成都）有限公司

任昊	4	特聘副研究员	四川大学	四川大学
张小松	5	教授	电子科技大学	电子科技大学
冯佳坤	6	AI XDR产品线总经理	亚信科技（成都）有限公司	亚信科技（成都）有限公司
刘东红	7	高级副总裁		
汤殿华	8	高级工程师	中国电子科技集团公司第三十研究所	中国电子科技集团公司第三十研究所
曾晟珂	9	教授	西华大学	西华大学
钱心缘	10	特聘副研究员	电子科技大学	电子科技大学

六、完成单位

排名	单位名称
1	电子科技大学
2	四川大学
3	西华大学
4	中国电子科技集团公司第三十研究所
5	亚信科技（成都）有限公司