# 前　言

作为关键生产要素,数据已成为数字化、网络化和智能化的基础,并推动了生活方式、生产方式和社会治理方式的深刻变革.考虑到数据滥用、数据泄露和权属纷争等风险,从数据流通、交易、使用、分配等环节全方位实现数据安全治理已成为一个至关重要且亟待解决的问题.为打造安全可信数据要素环境,应对区块链和人工智能等应用环境中日益加剧的安全挑战,探索数据要素安全的前沿与进展成为了学术界和工业界广泛关注的热点.

为进一步推动我国学者在数据要素安全领域的研究,及时报道我国学者在数据要素安全方面的最新研究成果,《计算机研究与发展》组织策划了“数据要素安全”专题.本专题通过公开征文共收到稿件72篇,从多个方面阐述了数据要素安全关键理论与技术,呈现了具有重要意义的研究成果.本专题严格按照《计算机研究与发展》的审稿要求进行,邀请了多位相关领域的专家参与评审,历经盲审、复审、终审等阶段,最终16篇论文入选本专题.这16篇论文分别涵盖数据要素安全流通、基于区块链的数据隐私保护和面向数据要素的人工智能安全等研究内容,在一定程度上反映了数据要素安全领域的最新研究成果.

## 1　数据要素安全流通

针对工业控制网络面临的复杂多变的安全威胁,王泽鹏等作者的“动态决策驱动的工控网络数据要素威胁检测方法”提出了一种基于深度强化学习和数据增强的威胁检测手段,解决现有方法对单一异常类型敏感的问题,从而提高了工业控制系统中威胁检测的准确率和鲁棒性.针对数据在跨域流转过程中易损毁和难嵌入的问题,李浩波等作者的“基于数据集蜜点的抗损毁数据标识技术”提出了一种基于数据集蜜点的抗损毁数据标识方法,有效提高了数据标识的鲁棒性和与原始数据的耦合度,保障跨域数据流转中的安全性和可靠性.针对云原生数据库在处理海量数据流时无法快速提取关键信息的问题,王修君等作者的“基于采样的数据流差分隐私快速发布算法”提出了一种数据流采样草图结构,通过对滑动窗口内数据进行采样统计和不合理数据过滤,实现了关键信息的快速提取和实时可用性.针对隐私保护基因序列分析方法效率低下问题,胡云舒等作者的“轻量级多用户可验证隐私保护基因序列分析方案”提出了一套可验证多密钥同态数据封装机制和一种轻量级的可验证隐私保护基因序列分析方案,能有效保护用户基因数据集和分析结果的隐私.针对已有云存储完整性校验机制无法在保护轻量级端侧数据机密性的前提下实现端侧多次任意验证的问题,韩冰等作者的“面向轻量级设备的云存储场景数据完整性校验方案”提出了一种基于可信执行环境的完整性校验机制,在保证数据隐私性的前提下实现了对云侧存储数据的即时验证.针对现有机密计算平台缺少运行时完整性保护的问题,李为等作者的“基于动态完整性度量的机密计算运行时监控方案”提出了一种通过向可信执行环境中引入控制流和数据流度量的动态完整性度量方法,从而实现了机密计算环境中用户工作负载的运行时完整性保护.

## 2 基于区块链的数据隐私保护

考虑到智慧医疗场景中医疗数据共享面临的隐私和安全问题，宋文鹏等作者的“基于分布式数字身份的可审计医疗数据共享”提出了一种基于区块链和代理重加密的去中心化身份模型，实现数据的安全流转与隐私保护，并简化了跨机构的数据处理流程.针对口令认证需要借助服务器存储账号和口令而带来的数据泄露隐患，柯宇泓等作者的“基于区块链的高效无口令认证方案”提出了一种基于区块链的多平台兼容高效无口令身份认证方案，实现了多平台互通、低开销、大规模用户适用的身份认证，提高了系统的安全性与透明度.针对区块链中因网络动态性强和管理困难而导致的DDoS攻击和账户接管等异常现象，朱龙隆等作者的“基于近似测量算法Sketch的高精度区块链异常检测机制”提出了一种异常交易账户检测方法，实现了对跨区块异常账户的准确检测.针对跨联盟链中数据隐私泄露、数据欺诈和支付抵赖等安全威胁问题，张川等作者的“面向跨联盟链的隐私保护数据要素交易审计方案”提出了一个面向跨联盟链的隐私保护数据要素交易审计方案，利用中继链上的智能合约实现了数据验证和支付管理.针对数据要素在区块链上流通效率低下的问题，李振宇等作者的“面向数据要素安全流通的区块链数据加速交换方法”提出了一种区块链数据加速交换手段，实现包括位置智能合约、聚合数据上传和优化的下载机制，不仅提升了区块链处理大规模数据的能力，还提高了数据流通的安全性和可靠性.针对跨域数据交易面临的一致性、可用性、合规性等问题，郝嘉琨等作者的“基于去中心化身份的跨域数据交易系统”提出了一种身份跨域解析机制，为跨域数据交易系统提供了安全与合规的解决方案.该机制支持基于身份属性的细粒度监管，并保证了跨域数据交易的原子性.

## 3 面向数据要素的人工智能安全

针对深度神经网络模型容易被盗窃和篡改等问题，金彪等作者的“基于水印技术的深度神经网络模型知识产权保护”提出了一种基于水印技术的知识产权保护方法，通过嵌入鲁棒水印和脆弱水印两种水印，实现了对模型版权的声明和完整性的验证.针对联邦学习中模型容易受到后门攻击的问题，刘嘉浪等作者的“基于联邦学习场景下与后门攻击的防御算法研究综述”从分布式学习的安全性和鲁棒性角度出发，阐明了联邦学习环境中特有的安全挑战，系统地综述了后门攻击及其对应的防御策略，并提出了可能的研究方向.考虑到人工智能模型面临的安全攻击风险，秦臻等作者的“面向人工智能模型的安全攻击和防御策略综述”对人工智能模型的安全性进行了系统深入的综述和分析，探讨了现有针对人工智能模型的攻击原理和技术现状，总结分析了常用的攻击检测方法和防御技术，并阐述了人工智能技术的主要安全挑战和未来展望.考虑到现有的数据遗忘方法在遗忘效果和模型泛化能力之间难以找到平衡点的问题，殷昱煜等作者的“基于特征约束和自适应损失平衡的数据遗忘方法”结合特征约束和自适应损失平衡的思想提出了一种近似遗忘框架，用于在“遗忘”特定数据和“恢复”模型泛化性能之间实现平衡，有效地保护了模型的泛化性能，并避免了“过度遗忘”或“过度恢复”等单一任务的过度影响.

本专题的顺利出版离不开各位作者、审稿专家和编辑部等方面的全力支持和无私贡献，我们对此致以诚挚的感谢.数据要素安全研究是一个发展迅速且活跃的领域，学科前沿的瞬息万变给特邀编辑和审稿人的审稿、选稿工作带来了巨大挑战.在审稿过程中难免出现不尽人意之处，恳请各位作者和读者理解和包容，同时也请各位同行不吝批评和建议.本专题的出版期望能给广大相关领域研究人员带来启发和帮助.

我们要特别感谢《计算机研究与发展》编委会和编辑部，从专题的立项到征稿启事的发布，从审稿专家的邀请到评审意见的整合，以及最后的定稿、修改和出版工作，都离不开他们辛勤和专业的付出.

最后，再次衷心感谢各位作者、审稿专家、特邀编委和编辑部的辛勤工作！

秦志光（电子科技大学）
翁 健（暨南大学）
熊 虎（电子科技大学）
陈大江（电子科技大学）
2024 年 8 月