大数据安全与隐私计算

Big Data Security and Privacy Computing

客座编辑

凌捷（1964- ），男，博士，广东工业大学计算机学院教授（二级）、博士生导师，兼任广东省大数据安全与服务工程技术研究中心主任、广东省电子政务信创企业重点实验室学术委员会主任等职。主要研究方向为网络信息安全、大数据安全、人工智能安全等，出版相关学术论著4部，在国内外重要期刊和国际会议上发表学术论文100多篇，获授权发明专利超过60件，获广东省科学技术奖一等奖1次、广东省科学技术奖二等奖2次，获南粤教书育人优秀教师等称号。

导读

社会发展进入了数字时代，数据被誉为新时代的石油，是企业和个人的宝贵资产。随着数据的不断增长和应用的不断普及，数据安全和隐私保护面临前所未有的挑战，大数据应用面临的数据安全威胁与隐私泄露严重破坏了正常的社会经济秩序，大数据平台抵御安全风险的能力亟须加强。隐私计算可在保护数据本身不对外泄露的前提下实现对数据的分析计算，达到数据“可用不可见”的目的。目前以多方安全计算、联邦学习、可信执行环境等为代表的隐私计算技术研究，彰显了其在充分保护数据和隐私安全的前提下，实现数据价值转化和释放的巨大潜力。

本刊以“大数据安全与隐私计算”为主题进行征文，旨在集中展示大数据安全与隐私计算中的大数据平台攻击检测、行业大数据应用安全、联邦学习中的数据安全与隐私保护、隐私计算与区块链、隐私计算的行业应用场景等方面的最新研究成果。本专题最终录用4篇文章，涵盖了大数据安全治理、数据交易的隐私安全、隐私计算可信网关、安全多方计算技术应用等领域的关键技术。

程伟等在《大数据技术在数据安全治理中的应用》中，结合大型央企的数据安全治理实践，凝练出应用中的关键技术问题，提出基于图算法的重点权限人员识别方法、基于生成对抗网络的用户与实体行为异常检测方法，设计、开发了数据安全治理平台，在降低数据安全风险、辅助企业合规建设、促进数据开发利用等方面起到了重要作用，在大型企业的大数据安全治理方面具有较好的应用推广价值。

金加和等在《基于多方安全计算的公共数据融合创新模式研究及应用》中，针对公共数据领域提出了基于多方安全计算的公共数据融合创新模式，分析了模式中多方安全计算核心系统的3个子层——联合计算子结构层、安全关系代数层和多方安全计算基础算子层，通过技术创新突破制度制约，兼顾数据价值提升和数据安全保障，并设计了在保护数据安全的前提下利用各主体公共数据联合计算的技术架构，给出了实现公共数据融合创新模式的通用流程，讨论了公共数据融合创新模式的应用实例，可为畅通数据资源大循环提供新模式的借鉴。

叶剑等在《支持互联互通的隐私计算网关设计与实现》中，从系统架构的视角阐述隐私计算互联互通技术的“应用层、协议层、通信层”三层次实现路径，针对目前隐私计算互联互通平台计算原理复杂、架构多样化等特点，提出Adaptation机制互联互通框架，解决了不同架构的兼容问题。通过传统机器学习、横向联邦、纵向联邦的具体实验场景，验证了所提的隐私计算互联互通可信网关的有效性和合理性。

为了确保感知数据交易的可靠性和隐私安全，陈家辉等在《基于区块链的感知数据交易隐私保护方案》中，提出了一个基于混洗差分隐私的区块链感知数据交易方案。该方案不需要可信的第三方，数据消费者可通过区块链交易平台发布任务并进行广播，进行安全隐私的数据交易，可实现接近中心化差分隐私的隐私保护效果。

大数据安全与隐私计算是当前的热点研究方向。本专题录用的文章略侧重于关键技术的场景应用。期待这些研究工作能够推动学术界和产业界在大数据安全和隐私计算领域的融合创新，为数字中国建设提供安全关键技术支持。