

数据安全

Data Security

客座编辑



罗圣美（1971—），男，博士，中孚信息股份有限公司高级副总裁、研究员级高级工程师，多年从事通信网络、云计算、大数据、人工智能、数据安全等核心技术和产品研制工作，突破分布式、大容量和高性能等多项关键技术，在电信、金融、能源和智慧城市等领域获得规模商用。主持国家科技重大专项、高质量发展专项和省级重点研发计划项目10余项，荣获国家科技进步奖二等奖1项、省部级科技进步奖一等奖4项，参与制定国际、国家及行业标准9项，发表论文60余篇，授权发明专利50余项。



凌捷（1964—），男，博士，广东工业大学教授（二级）、博士生导师、原计算机学院院长，广东省人民政府“数字政府”改革建设专家委员会委员，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。主要研究方向为网络信息安全、智能视频处理技术等。出版相关学术论著4部，发表学术论文100多篇，获授权发明专利超过60项，曾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、中国产学研合作创新成果一等奖、广东省南粤教书育人优秀教师等奖励。

导读

我国数字经济已进入快车道，各行业数字化转型加速推进。在自然资源、智慧金融、数据交易等领域，数据驱动的新业态、新模式不断涌现。尽管数字经济前景广阔，但数据安全风险不容忽视。一方面，数据泄露、滥用、非法交易事件频发；另一方面，跨境数据流动、人工智能伦理、隐私保护等问题日益复杂化。同时生成式人工智能技术的快速发展使数据合规使用面临新的挑战。

为应对数据安全挑战，我国已构建了较完善的数据安全治理体系。《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》共同构成数据安全治理的“三驾马车”，明确了数据分类分级、重要数据出境安全评估、个人信息最小化收集要求。《促进和规范数据跨境流动规定》进一步细化了数据出境规则，在保障数据安全的前提下促进国际数据合作。

《大数据》一直致力于推动大数据领域的学术交流与技术进步，为了深入探讨和分享数据安全领域的最新研究成果，本刊组织“数据安全”专题，最终录用的4篇文章基于不同研究方法和应用领域开展研究，涵盖了数字水印技术、人机信任机制、数据跨境流动和自然资源保护等一系列关

键基础主题。

在技术研究方面，张旭龙等人设计了一种基于可逆网络用于高效定位的双嵌入水印模型，在鲁棒性训练中引入了可逆神经网络，提高了模型的合理性和稳定性，具有更高的容量和更有效的定位能力。在信任机制方面，罗中岩等人提出了一种通用的U-XAI人机信任机制及治理框架，旨在解决人工智能领域中“社会技术鸿沟”带来的信任问题，提升人工智能系统可信度，为人工智能的可信治理提供了参考。在数据跨境流动方面，蒋荣等人提出了一种基于智能合约的数据跨境流动多方互信机制，基于区块链去中心化、难篡改特性，构建了覆盖身份验证、合规审查、责任追溯的全流程解决方案，提升数据流动透明度与安全性。在自然资源保护领域，魏立力等人研究了提升自然资源数据应用效率与保障数据安全方面的实施路径，在组织架构、制度规范和技术支撑等方面，提出了加强数据管理与安全保护的优化思路。

数据安全技术研究和产业应用是一个持续迭代、相互促进的过程，本刊将继续关注最新的技术发展和创新应用，推动构建发展与安全并重的数据生态，助力数字中国蓬勃健康发展！