前　言

云计算、区块链、人工智能与边缘计算等技术的协同演进，正推动网络与系统架构从集中式向分布式加速跃迁. 新型分布式网络与系统凭借其多中心化与去中心化融合的信任机制、云—边—端协同的智能处理能力，以及分布式数据库与无服务器架构的灵活扩展性，已成为构建未来数字基础设施的核心范式. 从工业物联网的跨域协作到区块链赋能的数字钱包，从联邦学习驱动的分布式人工智能到低时延 Agentic 网络的实时决策，分布式技术正深刻地重塑金融、制造、医疗等关键领域的应用生态.

然而，分布式系统的开放性与去中心化特性，也使其面临前所未有的安全挑战：数据流动的跨域性削弱了传统边界防护的有效性，多主体协同机制扩大了攻击面，资源受限设备进一步加剧了安全防护的复杂性. 如何在保障系统高效性与可用性的前提下，构建覆盖“数据全生命周期”与“系统全栈”的动态安全防护和隐私保护体系，已成为制约新型分布式技术规模化落地的关键瓶颈.

为进一步推动我国学者在新型分布式网络与系统中的数据安全与隐私保护领域的研究，《计算机研究与发展》特别策划“新型分布式网络与系统中的数据安全与隐私保护”专题. 本专题通过公开征文共收到稿件 41 篇，从多个方面阐述了新型分布式网络与系统中的数据安全与隐私保护关键理论与技术，呈现了具有重要意义的研究成果. 本专题的审稿严格按照《计算机研究与发展》期刊的审稿要求进行，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 8 篇论文入选本专题. 这些论文分别涵盖区块链赋能的分布式安全与信任增强方法、分布式系统中的新型攻击技术、分布式人工智能安全训练框架、分布式系统中的异常检测方案等研究内容，集中展示我国学者在该领域的最新突破.

1　区块链赋能的分布式安全与信任增强方法

李哲成等作者的“基于区块链的轻量级工业物联网跨域认证与数据共享方案”提出了基于区块链的轻量级认证与数据共享架构. 该架构通过引入分布式密钥生成技术构建服务密钥，并设计轻量级消息认证算法，在保障设备匿名性与数据保密性的同时，将资源消耗降低 40% 以上，为分布式工业系统提供了可扩展的安全通信框架. 邓智洪等作者聚焦区块链轻客户端协议的存储与通信瓶颈，提出了“DecXClient: 一种通用、安全的轻客户端协议”. 该协议通过链质量属性驱动的动态验证集选举机制，结合加权多重签名证明生成范式，在不依赖可信第三方的前提下，将状态证明大小压缩至 1 248 B，验证延迟趋近于零，有效抵御 Eclipse 攻击，为跨链通信与数字钱包轻量化提供了安全基石.

2　分布式系统中的新型攻击技术

吴震等作者的“SM4 密钥扩展算法的单能迹攻击”针对分布式物联网中 SM4 密码算法，

提出了基于贝叶斯网络的单能迹的侧信道攻击方法.该攻击方法通过构建概率图模型与置信传播算法,在信噪比仅 10 dB 的噪声环境下实现 70% 的主密钥恢复成功率,较传统多能迹攻击方法的效率提升 3 倍,为轻量级设备密码实现提供了侧信道防护理论依据.丁熠等作者的“针对 SAM 下游模型脆弱模块的对抗迁移攻击”针对视觉基础模型 SAM（segment anything model）在下游任务中的对抗脆弱性,提出了基于特征相似度的脆弱模块迁移攻击方法.该方法通过识别 SAM 编码器中最易受攻击的 Transformer 模块,并结合梯度稳健损失消除梯度差异,在医学分割、阴影分割等任务中使模型性能下降超 60%,揭示了分布式视觉系统中的潜在安全风险.

3 分布式人工智能安全训练框架

闫彩虹等作者的“BTFAT:突破联邦对抗训练中鲁棒性与准确性权衡的框架”针对联邦学习模型在对抗样本攻击下的脆弱性,提出了面向联邦对抗训练的鲁棒性与准确性权衡框架.该框架通过决策空间收紧算法缩小类内样本距离、扩大类间样本距离,并设计权重惩罚优化算法约束本地模型偏离,突破了干净样本准确性与对抗鲁棒性的权衡困境,在非独立同分布数据集上实现鲁棒性与准确性的协同提升,为分布式人工智能安全训练提供了新范式.

4 分布式系统中的异常检测方案

周颖杰等作者的“一种云平台中的异常检测轻量化模型智能构建方案”针对云平台异常检测模型构建依赖专家知识的问题,提出了轻量化模型智能构建方案.该方案通过特征自动生成、优化与模型超参数调优,支持医学云、金融云等异构场景下的异常检测任务,模型构建效率提升 70%,检测准确率达 95%,为云服务安全运维提供了低门槛解决方案.张锋等作者的“低时延智能体网络中基于三阶段关联验证的伪造链路攻击检测”提出的方案通过时延转换、多径传输模拟与极值理论阈值分析,有效缓解测量误差的影响,在背景流量干扰下仍保持 92% 的检测准确率,为分布式实时系统的链路安全提供了关键技术支撑.李冬芬等作者的“融合联邦学习与量子卷积神经网络的入侵检测模型”提出的模型通过量子比特复用技术提升资源利用率,并利用联邦学习实现多客户端协同建模,在分布式物联网入侵检测中的误报率降低至 5% 以下,为异构数据隐私保护与高维稀疏特征建模提供了创新思路.

上述研究不仅展现了我国学者在分布式安全领域的系统性创新,更体现了从底层密码学突破到系统级安全架构设计的全链条攻关能力.我们期待,本专题能成为连接学术研究与产业实践的桥梁,激发更多学者投身于新型分布式系统安全领域的研究,共同守护数字时代的“安全基座”,为全球网络安全治理贡献中国智慧与中国方案.

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.新型分布式网络与系统中的数据安全与隐私保护研究是一个发展迅速且持续活跃的领域,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）
何德彪（武汉大学）
秦 臻（电子科技大学）
陈大江（电子科技大学）
2025 年 7 月