计算机科学
COMPUTER SCIENCE

数据安全专题序言

郝志强, 李俊, 陈立全, 王佰玲, 孙建国, 张立国

引用本文

郝志强, 李俊, 陈立全, 王佰玲, 孙建国, 张立国. 数据安全专题序言[J]. 计算机科学, 2023, 50(9): 1-2.

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.qy20230901

数据安全专题序言

郝志强[1,2]　李　俊[2]　陈立全[3]　王佰玲[4]　孙建国[5]　张立国[6]
1 工业和信息化部教育与考试中心　北京 100040
2 国家工业信息安全发展研究中心　北京 100040
3 东南大学　南京 210096
4 哈尔滨工业大学(威海)　山东 威海 264209
5 西安电子科技大学　西安 710126
6 哈尔滨工程大学　哈尔滨 150001

数据安全指保护数据免受未经授权的访问、泄露、篡改、破坏或丢失的过程和措施。在数字化时代,数据已经成为各种组织和个人生活中不可或缺的资产。在面临着持续不断的威胁和挑战的背景下,我们汇集了一系列关于网络与数据安全领域的前沿创新研究,旨在探索新的方法、技术和策略来降低数字世界的风险,保护其免受侵害。本专题涵盖了多个重要主题,包括数据安全与加密、网络攻击和防御、隐私保护与数据分析等,共收录了10篇文章,其中包括2篇综述性文章和8篇技术性文章。每篇文章都从不同角度深入探讨了当今网络与数据安全领域的关键问题,并提出了具有实际应用价值的解决方案。

在数据安全与加密方面,本专题共收录了3篇文章。《轻量级分组密码算法综述》概述了轻量级分组密码算法的研究现状和进展,按算法结构将其分为六大类并进行了详细描述,使用多维度评价指标综合比较软硬件实现,深入探讨了安全性、资源开销和性能。《基于区块链的云上数据访问控制模型研究》介绍了区块链与基于密文策略的属性加密相结合的方案在云上数据访问控制中的广泛应用,提出了一个基于区块链的解决方案,结合智能合约、多属性授权和DMA-ABS方案实现了细粒度访问控制和匿名性身份验证,最终在Hyperledger Fabric上实现了访问控制流程。《基于SecureCNN的高效加密图像内容检索系统》提出了基于近似数同态的高效加密图像检索方案,通过同态神经网络特征提取和分级可导航小世界算法构建索引,实现了高效的图像检索,同时保证了数据安全。

在网络攻击和防御方面,本专题共收录了3篇文章。《基于分层任务网络的攻击路径发现方法》提出了一种基于分层任务网络的攻击路径发现方法,通过引入多层级K路划分算法、专家经验融合路径规划和局部信息维护方案,解决了路径生成性能差、领域问题描述难和路径更新效率低的问题。《基于生成对抗网络与变异策略结合的网络协议漏洞挖掘方法》提出了一种基于生成对抗网络与变异策略结合的网络协议漏洞挖掘方法,利用生成对抗网络缓解协议构造测试用例的不客观性问题,设计指导性变异策略来提高模糊测试效率,提升了工控网络协议漏洞挖掘的有效性与效率。《深度神经网络的后门攻击研究进展》概述了神经网络后门攻击的威胁模型,然后将神经网络后门攻击分为基于投毒的后门攻击和无投毒的后门攻击两大类,对神经网络后门攻击的发展进行了梳理和总结,对现有资源进行了汇总,并对后门攻击未来的发展趋势进行了展望。

在隐私保护与数据分析方面,本专题共收录了4篇文章。《抗推理攻击的隐私增强联邦学习算法》提出了一种抗推理攻击的隐私增强联邦学习算法,通过优化问题构建和新特征生成,解决了梯度传递引起的数据隐私泄漏问题,有效提升了网络模型的隐私保护能力。《面向流程工业控制的双安融合知识图谱研究》提出了一种基于双安融合知识图谱的方法,基于BERT的命名实体模型和图对齐等技术,从工控领域的网络安全数据库和实际化工生产文档中提取实体和关系,构建了流程工业双安融合知识图谱,为工控系统提供了综合的安全保障。《面向智能视频监控的人体小目标检测》提出了一种名为尺度分布搜索的优化策略,通过高斯模型对数据集目标的尺度分布进行建模,并通过迭代寻找最优分布参数,最终结合目标特征分布与检测器性能,实现了更好的目标检测性能。《基于自适应遗传算法的微服务移动目标防御策略》提出了一种名为动态轮换策略的基于自适应遗传算法的微服务移动目标防御策略,通过微服务特点分析攻击路径,利用微服务攻击图模型建模攻击场景,并使用AGA求解最优安全配置,有效提升了防御回报率。

本专题将上述论文呈现给感兴趣的计算机科学研究者,希望为其带来一些启发。

郝志强　研究员,工业和信息化部教育与考试中心主任、书记,享受国务院政府特殊津贴。担任国家工业控制系统与产品安全质量监督检验中心主任,工信部工业信息安全感知与评估技术重点实验室主任,工信部工业领域数据防护与安全测评重点实验室主任,全国工业和信息化职业教育教学指导委员会副主任委员,全国工业和信息化职业教育教学指导委员会计算机分委会主任委员,中国电子学会网络空间安全专委会副主任委员,中国网络信息安全科技创新发展联盟副理事长/专家等。担任中央网信办、教育部“一流网络安全学院建设示范项目高校”评审专家,工信部启明计划评审专家,工信部经济系列正高级职称评审委员会主任,商务部援外项目评审专家,学术期刊《工

业信息安全》主编等。长期致力于网络空间安全、工业信息安全、两化融合、新一代信息技术等的科学研究，重大项目工程建设和产业推进工作，主持国家重点研发计划、国家重大科技项目计划、国防科技工业基础科研、工信部工业互联网创新发展工程等重大专项20余项，公开出版发表学术论文40余篇、个人著作5部、国家技术发明专利20余项，获中国电子学会、中国石油和化工自动化应用协会等科技进步奖，全国高校毕业生就业工作先进个人，航天人才贡献奖等国家级、省部级奖励18项(次)。

李 俊 国家工业信息安全发展研究中心首席专家、保障技术所所长，工学博士、正高级工程师，工业领域数据保护与安全测评工信部重点实验室副主任。长期从事工业领域网络和数据安全研究与支撑保障工作，作为核心起草者参与国家工控安全、工业数据安全、工业数据安全等10余项政策文件制定工作。担任30余个国家重大、重点项目的负责人/技术总师，牵头建设的多个平台已成为我国工业领域网络和数据安全保障工作的重要支撑系统。已发表学术论文55篇，主编技术专著2部，获授权技术发明专利27项，获省部级科技奖励一等奖2项、二等奖1项、三等奖1项。

陈立全 教授、博导，国家重点研发计划项目首席科学家，东南大学网络空间安全学院副院长，华英青年学者，江苏省科技咨询专家，全国信息安全标准技术委员会委员；入选江苏省第九批“六大人才高峰”，江苏省“333高层次人才培养工程”培养对象；江苏计算机学会副秘书长，信息安全专委会主任，工控安全专委会副主任，江苏省网络空间安全高校联盟秘书长，江苏省网络空间安全学会常务理事，密码学会常务理事，《网络与信息安全学报》编委。承担并完成了国家重点研发计划、“863”计划、国家自然科学基金、博士后基金、省部级基金等项目40余项，曾获中国通信学会三等奖和江苏省通信学会一等奖等。在国内外重要期刊及IEEE国际学术会议上发表学术论文100余篇，其中SCI收录近50篇，已获得授权发明专利近20项，承担IEEE权威国际期刊及会议的编审工作。

王佰玲 哈尔滨工业大学教授，博士生导师，国家高层次人才，山东省网络空间安全工程技术研究中心主任，山东省网络空间安全高校重点实验室主任。主要研究领域为网络空间安全，包括信息对抗技术、网络攻防技术、网络信息搜索技术、工业控制网络及系统安全、车联网安全技术研究等。完成大规模网络流量分析平台、互联网舆情分析平台、工业物联网安全检测平台、工业互联网安全通信平台等多个平台建设；先后主持及参与国家自然科学基金、国家重点研发计划等课题7项，其他省部级课题40余项；在国内外期刊及会议上发表信息安全领域高水平论文100余篇。

孙建国 教授、博导，国家重点研发计划项目首席科学家，浙江省高层次领军人才，西安电子科技大学杭州研究院工程中心主任，信息安全共性技术国家工程研究中心总工程师，天地一体信息技术国家重点实验室客座教授。担任《网络空间安全》《计算机教育》《信息网络安全》《无线电工程》等中文核心杂志编委，以及 *Ad Hoc Networks*，*IEEE Transactions on Information Forensics and Security*，*Review for Expert Systems With Applications* 等15个国外期刊特邀审稿专家。承担并完成了国家重点研发计划、国防基础科研、军委科技委重点项目等20余项。主要从事工业信息安全、智能安全等方面的研究工作。

张立国 哈尔滨工程大学副教授、博士生导师，计算机学院软件工程中心主任。中国计算机学会高级会员，中国电子学会会员，中国人工智能学会委员，YOCSEF哈尔滨分论坛优秀学术委员；国家工业信息安全发展中心高级顾问，恒安嘉新科技股份公司外部专家，航天海鹰钛业有限公司科技顾问。研究方向为机器学习与人工智能、数字图像处理、多媒体数据处理、智能软件及其安全等。多次承担国家/省/市的自然科学基金项目、重点研发计划、863/973计划、科技攻关项目等。累计发表SCI论文30余篇，申请国家专利20余项，获省部级科技奖励3项，出版教材/专著3部。