第五届新兴信息安全与应用国际会议

The 5-th International Conference on Emerging Information Security and Applications

EISA • 2024

承办单位

江苏理工学院

会议时间：2024 年 10 月 18 日-10 月 19 日

会议地点：明都国际会议中心（常州西太湖）

会务组联系方式：

周元健　手机：18589942150

赵全玉　手机：18851113718

会议联合主席

Weizhi Meng, Technical University of Denmark, Denmark

组织委员会

General Chairs

Zhengjun Jing, Jiangsu University of Technology, China

Weizhi Meng, Technical University of Denmark, Denmark

Sokratis Katsikas, Norwegian University of Science and Technology, Norway

Program Chairs

Wenjuan Li, The Education University of Hong Kong, Hong Kong SAR, China

Liqun Chen, The University of Surrey, UK

Javier Lopez, University of Malaga, Spain

Publicity Chairs

Quanyu Zhao, Jiangsu University of Technology, China

Youqian Zhang, The Hong Kong Polytechnic University, China

Na Ruan, Shanghai Jiao Tong University, China

Publication Chair

Peizhong Shi, Jiangsu University of Technology, China

Web Chair

Wei-Yang Chiu, Technical University of Denmark, Denmark

Steering Committee

Jiageng Chen, Central China Normal University, China

Liqun Chen, University of Surrey, UK

Steven Furnell, University of Plymouth, UK

Sokratis K. Katsikas, Norwegian University of Science and Technology, Norway

Javier Lopez, University of Malaga, Spain

Weizhi Meng, Technical University of Denmark, Denmark

Conference Schedule

October 18, 2024	Friday	**Mingdu International Conference Center**
08:00-18:00	Registration	
October 19, 2024	Saturday	**Mingdu International Conference Center**
08:30-09:00	Welcome General/Program Chairs	
Session 1: Keynote Speak Session Chair: Weizhi Meng, Technical University of Denmark		
09:00-09:30	Secure Data Sharing in Internet of Vehicles	Lei Zhang
09:30-10:00	Integrated security protection system and key technologies for Intelligent Connected Vehicles	Jie Cui
10:00-10:20	Tea Break	
10:20-10:50	Testing Learning-Enabled Cyber-Physical Systems: Current Approaches and Future Directions	Xi Zheng
10:50-11:20	EEG based Authentication: State-of-the-art and Future Directions	Weizhi Meng
Session 2: Federated Learning Session Chair: Zhengjun Jing		
11:20-11:35	Comparative Study of Machine Learning Approaches for Phishing Website Detection	Mingwu Zhang, Chukwuebuka Amandi Ogbebisi and Bingbing Li
11:35-11:50	Privacy Optimization of Deep Recommendation Algorithm in Federated Framework	Xiaopeng Zhao, Xiao Bai, Guohao Sun and Zhe Yan
11:50-12:05	Adaptive Differential Privacy Based Optimization Scheme for Federated Learning	Qi Yuan, Ershuai Xu, Hao Yuan and Shuo Zhao
12:05-13:30	Lunch Break	
Session 3：Federated Learning and Blockchain Session Chair: Peizhong Shi		
13:30 - 13:45	Research on Key Technologies of Fair Deep Learning	Xiaoqian Liu Weiyu Shi

13:45 - 14:00	GPT-based WebAssembly Instruction Analysis for Program Language Processing	Liangjun Deng, Qi Zhong, Hang Lei, Yao Qiu and Jingxue Chen
14:00 - 14:15	DefMPA: Defending Model Poisoning Attacks in Federated Learning via Model Update Prediction	Mengya Guo, Bing Chen, Baolu Xue and Jiewen Liu
14:15 - 14:30	Cascading failures model with noise interference in supply chain networks	Bo Song, Yi Qin, Yu-Rong Song and Xu Wang
14:30 - 14:45	Blockchain-based key management scheme in Internet of Things	Zihan Wang, Jiqun Zhang, Jingcheng Song, Yongwei Tang and Hongyuan Cheng
14:45 - 15:00	Delegated Proof of Stake Consensus Mechanism Based on the Overall Perspective of Voting	Chengtang Cao, Shupei Mo and Zongzheng Huang
15:00 - 15:15	Tea Break	
Session 4: Data Security **Session Chair: Quanyu Zhao**		
15:15 - 15:30	Attribute-Based Secret Key Signature Scheme	Chengtang Cao,Zongzheng Huang and Shupei Mo
15:30 - 15:45	Digital token transaction tracing method	Ling-Ling Xia, Qun Wang, Zhuo Ma and Bo Song
15:45 - 16:00	High-Efficiency Phase-Index Correlation Delay Shift Keying Modulation	Junyi Duan, Hua Yang, Chenkai Tan and Tianci Zhao
16:00 - 16:15	A Privacy-Preserving and Fault-Tolerant Data Aggregation Scheme in Smart Grids	Yongkang Zhu
16:15 - 16:30	Local Differential Privacy for Key-Value Data Collection and Analysis Based on Privacy Preference and Adaptive Sampling	Zhengyong Zhai,
16:30 - 16:45	A Distributed Privacy-preserving Data Aggregation Scheme for MaaS Data Sharing	Lin Zhu
16:45 - 17:00	Exploring Interpretability in Backdoor Attacks on Image	Jiaxun Li, Yefeng Meng, Gaoyuan Zhou, MingxinXu, Hanwei Qian and Hao Chen
17:00 - 17:15	SDDRM: An Optimization Algorithm for Localized Differential Privacy Based on Data Sensitivity Differences	Bingbing Li, Peizhong Shi, Chunsheng Gu, Yan Zhang and Zhengjun Jing
17:15 - 17:30	Closing Remarks	General/Program Chairs

特邀报告专家：

张磊，研究员，博导，博士毕业于西班牙 Universitat Rovirai Virgili, URV，随后在 URV 做博士后研究，现任华东师范大学软件工程学院副院长。留学期间，访问了荷兰 CWI 研究所。研究兴趣包括车联网/物联网安全，密码学，云计算安全，人工智能安全，区块链，隐私保护。发表学术论文 100 余篇，包括 IEEE Transactions on Information Forensics and Security、IEEE Transactions on Dependable and Secure Computing、IEEE Transactions on Computers 、 IEEE Transactions on Intelligent Transportation Systems 、 IEEE-ACM Transactions on Networking、ESORICS 2014、ASIACRYPT 2011 等国际期刊会议。担任中国密码学会青年工作委员会副主任，上海计算机学会信息安全专委会副主任。

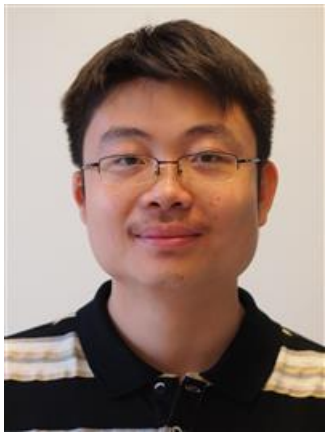
主持/参与国家/省部级等项目 20 余项，负责国家重点研发计划重点专项子课题两项，参与国家自然科学基金重点项目等。担任了多个国际期刊编委/客座编辑，100 多个国际会议程序委员会委员、40 多个国际期刊包括 IEEE Transactions on Information Forensics & Security 、 IEEE Transactions on Parallel and Distributed Systems 、 IEEE Transactions on Vehicular Technology、IEEE Transactions on Wireless Communications 的特邀审稿人。

崔杰，教授，博导，安徽大学计算机科学与技术学院副院长，安徽省物联网安全技术工程实验室副主任，国家自然科学基金联合基金重点项目负责人，安徽省杰出青年基金获得者，安徽省科研创新团队负责人，IEEE 高级会员。受聘 ACM 合肥分会副主席、国际期刊 IET Communications 编委，国际期刊 Security and Communication Networks 编委和客座编委，国际期刊 Sensors 和 Electronics 客座编委。担任 IEEE/ACM UCC 2020、IEEE/ACM BDCAT 2023 等 10 余个国际会议的 Publicity Chair 和 TPC。学术水平得到国内外同行的广泛认可，2020-2023 连续四年入选美国斯坦福大学发布的全球前 2%顶尖科学家“年度影响力”榜单。

近年来专注于车联网安全、物联网安全、区块链与密码学、人工智能安全、数字孪生安全等领域的研究，主持国家自然科学基金项目 5 项（其中重点项目 1 项）、安徽省杰出青年基金、安徽省高校协同创新项目以及企业委托项目 10 余项。创新性地构建了新型车联网安全架构与密钥管理机制，提出了高安全性的车联网认证与隐私保护方法，设计了面向物联网和车联网的轻量级密码算法，并探索关键技术理论在智能交通系统、工控网络系统等的应用推广。围绕上述内容开展深入研究，取得了一系列国际领先的科研成果，在 IEEE JSAC、IEEE TDSC、IEEE TIFS、IEEE TPDS、IEEE TMC、IEEE TC、中国科学: 信息科学等顶级期刊和会议发表论文 200 余篇，其中 CCF A 类论文 20 余篇，IEEE/ACM 汇刊 40 余篇，谷歌学术引用 5400 余次，H 指数 43，热点论文 1 篇，高被引论文 5 篇。获安徽省计算机学会科技进步二等奖（2021 年），国际会议 ProvSec 2023、IEEE/ACM RTDPCC 2020 最佳论文奖，安徽省计算机学会硕士学位论文优秀指导教师奖（2020 年，2021 年）。研发车联网身份认证与装备样机、安防联动和物联网安全服务等系统，在全国 20 多个城市部署，授权国家发明专利 30 余项，已转化应用 4 项。

郑曦博士于 2015 年获得德克萨斯大学奥斯汀分校软件工程博士学位。2024 年，他被授予澳大利亚研究委员会未来研究员。2005 年至 2012 年，他担任 Menulog Australia 的首席解决方案架构师。目前，他在澳大利亚麦考瑞大学担任多个领导职务：智能系统研究小组（ITSEG.ORG）主任、计算学院国际参与主任、高级讲师（相当于美国的副教授）、软件工程副项目负责人。他的研究领域包括网络物理系统测试和验证、安全分析、分布式学习、物联网和更广泛的软件工程。郑博士已成功获得澳大利亚研究委员会（1 名未来研究员、2 名链接和 1 名发现）和 Data61（CRP）项目的 240 多万美元竞争性资金，这些项目侧重于安全分析、模型测试和验证，以及为自动驾驶汽车开发值得信赖的人工智能。

他获得多个奖项，包括迪肯行业研究员奖（2016 年）和 MQ 早期职业研究员奖（2020 年亚军）。他的学术贡献包括众多被高度引用的论文和最佳会议论文奖。他曾担任领先的软件和系统会议的项目委员会成员，如 FSE（2022、2024）和 PerCom（2017-2025），并担任 IEEE CPSCom-2021 和 IEEE Broadnets-2022 的 PC 主席。此外，他还担任 ACM 分布式账本技术的副主编和施普林格可靠智能环境杂志的编辑。2023 年，郑博士是加州大学洛杉矶分校和德克萨斯大学奥斯汀分校的客座教授，也是值得信赖的自主网络物理系统国际研讨会的联合创始人。



蒙威志目前是丹麦技术大学（DTU） 应用数学和计算机科学系的副教授。他在中国香港特别行政区香港城市大学（CityU） 获得计算机科学博士学位。在加入 DTU 之前，他曾在新加坡 A*STAR 资讯通信研究所担任研究科学家。他目前是 DTU 的 SPTAGE 实验室主任。博士期间获得了杰出学术表现奖，并于 2014 年和 2017 年获得香港工程师学会 （HKIE） 青年工程师/研究人员杰出论文奖。他还多次获得国际会议的最佳论文奖和最佳学生论文奖，其他奖项包括 IEEE Blockchain 2018 和 IEEE ATC 2019 的 IEEE 杰出领导奖。他在 2020 年获得了 IEEE ComSoc 欧洲、中东和非洲地区（EMEA）最佳青年研究员奖，并在 2020 年获得了 IEEE MGA 青年专业人员成就奖，以表彰他对丹麦和第 8 区领导活动的贡献。

主要研究兴趣是区块链技术、网络安全和安全人工智能，包括入侵检测、区块链应用、智能手机安全、生物识别身份验证、人机交互安全、云安全、信任管理、恶意软件检测、网络物理系统安全和物联网安全。他还对应用密码学表现出浓厚的兴趣。他担任 IEEE Transactions on Dependable and Secure Computing 、 Journal of Information Security and Applications 和 International Journal of Information Security 等的编辑职务，并担任许多知名会议的主席/程序主席，如 IEEE Globecom（CISS）2020、IFIPSEC 2022、ESORICS 2022、ACM CCS 2023 等。

EISA 2024

交通信息：

1.到达常州奔牛国际机场
线路一：乘坐机场大巴到常州汽车总站（26 元），乘坐地铁 1 号线到延政大道站下车（南夏墅方向，10 站），打车至太湖明都国际会议中心酒店（约 20-30 元）。
线路二：打车至至太湖明都国际会议中心酒店（约 70-100 元）。

2.到达常州北站
线路一：乘坐地铁 1 号线到延政大道站下车（南夏墅方向，19 站），打车至太湖明都国际会议中心酒店（约 20-30 元）。
线路二：打车至至太湖明都国际会议中心酒店（约 45-70 元）。

3.到达常州站
线路一：乘坐地铁 1 号线到延政大道站下车（南夏墅方向，10 站），打车至太湖明都国际会议中心酒店（约 20-30 元）。
线路二：打车至至太湖明都国际会议中心酒店（约 35-60 元）。