Workshop Proposal for IEEE MASS 2025

1. Full Name

Data Security and LLM Safety in Smart Systems (abbr: DLS)

2. Organizers

Name	E-mail	Affiliation and its location
Minghui Xu	mhxu@sdu.edu.cn	Shandong University, China
Yue Zhang	zyueinfosec@gmail.com	Shandong University, China
Qin Hu	qhu@gsu.edu	Georgia State University, USA
Shan Wang	shanwangsec@gmail.com	The Hong Kong Polytechnic University, China
Qinhong Jiang	qinhong.jiang@polyu.edu.hk	The Hong Kong Polytechnic University, China

3. Organizer Biography

Minghui Xu is currently a Professor in the School of Computer Science and Technology at Shandong University. His research focuses on designing scalable, highly secure and reliable systems (including blockchain, decentralized storage network, and AI infrastructures) by integrating cryptography for provable security with distributed architectures for scalability and fault tolerance. He has published papers on pretigious conferences and journals, including USENIX Security, IEEE INFOCOM, IEEE ICDCS, IEEE TMC, IEEE TC, IEEE TPDS, IEEE JSAC, IEEE TWC. He received the Best Paper Award of WASA 2020 and GAIIS 2024. He has chaired several prestigious conferences, serving as Publicity Chair for IEEE ICMC 2023-2024 and IEEE SmartCity 2024, while leading tracks as Track Chair for EAI WiSATS 2025, IEEE IPCCC 2022-2023, and IEEE FNWF 2023. He also contributes to editorial boards including IEEE Transactions on Computers and Elsevier High-Confidence Computing, while serving on program committees for flagship security conferences including ACM CCS, USENIX Security, and ACM AsiaCCS.

Yue Zhang is professor at Shandong University. Before joining Shandong University, he was an assistant professor at Drexel University's Computer Science department. His research primarily focuses on system security, specifically in the areas of IoT Security and mobile security. He has published more than 40 papers in security

conferences (e.g., USENIX Security, ACM CCS, and NDSS) and journals (e.g., TDSC, TPDS). He received a Best Paper Honorable Mention Award at ACM CCS 2022, NDSS Distinguished Reviewer and the Best Paper Award at 2019 IEEE International Conference on Industrial Internet. He has also served on the organization committees of the conferences (e.g., general chair of EAI ICECI, track chair for IEEE MSN and IEEE MASS) and technical program committee of the conferences (e.g., USENIX Security, NDSS, ACM CCS, RAID). He serves as an Associate Editor for IEEE T-IFS, HCC and Editor Member of the Blockchain Journal, Electronics Journal, and CMC. His research had led to the discovery of many vendor-acknowledged vulnerabilities, such as by Bluetooth SIG, Apple, Google, and Texas Instruments, and had attracted intense media attention such as Hacker News, and Mirage News.

Qin Hu is currently an Assistant Professor with the Department of Computer Science, Georgia State University (GSU). She received the Ph.D. degree in computer science from The George Washington University in 2019. Prior to joining GSU, she was an Assistant Professor with the Department of Computer and Information Science, Indiana University - Purdue University Indianapolis. She received the Best Paper Award of WASA 2020, the Best Paper Award Runner-up of IEEE MASS 2021, and the IEEE Outstanding Leadership Award as Publicity Chair of IEEE EUC 2022. She has served as the Editor and Guest Editor for several journals (e.g., ELSEVIER Journal of Network and Computer Applications, IEEE Transactions on Network Science and Engineering), the TPC/Publicity chair for several workshops/conferences (e.g., IEEE EUC’22), and the TPC Member for many international conferences (e.g., IEEE INFOCOM, IEEE Globecom, IEEE Blockchain). Her research interests include wireless and mobile security, data privacy, edge computing, federated learning, and blockchain.

Shan Wang is currently a Postdoctoral Fellow in the Department of Computing at The Hong Kong Polytechnic University. Her research interests include blockchain and cybersecurity, focusing on blockchain data security and user anonymity. Her papers have been published in leading conferences including INFOCOM and ICDCS, and she received a Distinguished Paper Award at IEEE ICDCS 2024. She has served on the organizing committees of six conferences, including as web co-chair for BCRA 2025, local organization and registration co-chair for ACM/IFIP Middleware 2024, organizing chair for the workshop STIM 2024, session chair for IEEE ICDCS 2024 and

MetaCom 2024, and publicity and social media chair for ICECI 2024. Additionally, she has participated in the technical program committees of nine conferences, such as ICC 2025, Middleware 2024-2025, MSN 2023-2024, ICBC 2024-2025, ICPADS 2024, MASS 2024 and so on.

Qinhong Jiang is currently a Postdoctoral Fellow in the Department of Computing at The Hong Kong Polytechnic University. His research aims to safeguard the security and privacy of cyber-physical systems, bridging the domains of embedded systems, sensing, mobile computing, and AI. His work has been published in top-tier conferences/journals, such as USENIX Security, NDSS, and IEEE TIFS. He has served on the organizing committees of EAI SecureComm 2025 and as a PC member/reviewer for conferences and journals, including RAID'25, ICC'25, and IoT-J.

4. Description

As smart systems integrate generative AI with edge-cloud architectures, their security paradigms face unprecedented challenges. Data security and LLM safety are crucial for trustworthy smart infrastructure. Data security protects sensitive information throughout its lifecycle, while LLM safety ensures the reliability and ethical alignment of AI behaviors. These two are intertwined: compromised data integrity directly undermines model robustness, and unsafe LLM outputs can lead to data breaches in interconnected smart ecosystems. This is especially critical in mobile environments with dynamic connectivity, resource constraints, and device diversity. Traditional frameworks, developed for static systems, are inadequate to address these dynamic, resource-constrained scenarios. The limitation is increasingly evident in real-world incidents across healthcare, transportation, and smart manufacturing sectors.

This workshop aims to unify data protection and AI safety for next-generation smart systems. While the main conference covers broader mobile ad-hoc network security, we specifically focus on emerging threats arising from the fusion of generative AI and distributed intelligence. Topics will span novel threat models, architectural safeguards, and evaluation methodologies that jointly strengthen data flows and AI behaviors. The outcomes will deliver practical guidelines to help academia and industry harness LLMs' transformative potential while mitigating systemic risks in critical applications like smart healthcare, autonomous transportation, and industrial IoT.

5. Target Audience

- Researchers in decentralized AI security and data-model co-security
- Practitioners deploying AI in IoT/edge environment
- Policy makers addressing AI ethics in smart infrastructure
- Cross-disciplinary communities (security + AI + edge systems)

6. Program Committee Member Candidates

Name	E-mail	Affiliation and its location
Akshita Maradapu Vera Venkata Sai	amaradapuveravenkatasai@towson.edu	Towson University, USA
Chonghe Zhao	zhaochonghe_szu@163.com	Nanyang Technological University, Singapore
Christopher Ellis	ellis.729@buckeyemail.osu.edu	Ohio State University, USA
Chunchi Liu	liuchunchi@gwu.edu	Huawei Technologies, China
Mario Michael Kubek	mkubek@gsu.edu	Georgia State University, USA
Qi Luo	luoqi4110217@hotmail.com	Hong Kong University of Science and Technology, China
Ruochen Zhou	zrccc@zju.edu.cn	The Hong Kong University of Science and Technology, China
Vishal Karande	vishalmkarande@gmail.com	Google, USA
Xiaodong Qi	xiaodong.qi@ntu.edu.sg	The Hong Kong Polytechnic University, China
Xiaoli Zhang	xiaoli.z@ustb.edu.cn	University of Science and Technology, China
Xiaoqian (Tiffany) Zhang	xiaoqianzhang@unomaha.edu	University of Nebraska Omaha, USA
Yan Long	yan.long@virginia.edu	The University of Virginia, USA
Yasra Chandio	ychandio@umass.edu	University of Massachusetts Amherst, USA

Yongshun Xu	yxu@neurologica.com	Samsung Neurologica Corporation, USA
Youming Tao	tao@ccs-labs.org	TU Berlin, Germany

7. Proposed Format

- **Duration of the workshop:** Half-day workshop (3.5 hours)
- **Session 1**: Keynote by top scholars in distributed AI security (40 min)
- **Session 2**: Peer-reviewed paper presentations (6 papers x 15 min)
- **Session 3**: Panel discussion: "Decentralized Intelligence: Can We Break the Paradox of Data-Model Co-Security?"
- **Session 4**: Lightning talks & open debate

8. Past Versions

N/A

9. Call for Papers

Topics:

We invite submissions on emerging challenges, including but not limited to:

- Anomaly Detection for Data Integrity in Smart Environment
- Federated Fine-Tuning with Data Provenance Tracking
- Dynamic Access Control and Data Security in Heterogeneous AI Systems
- Blockchain-enabled Decentralized AI Governance
- Incentive-Aware Security Protocols in Decentralized AI
- Byzantine-Robust Consensus for Mobile Model Sharing
- Adversarial Attacks and Defenses in Mobile Networks
- Model Extraction Attacks Against Edge-Deployed LLMs
- Jailbreaking Risks in Autonomous Decision Systems
- Security and Privacy of Distilled On-Device Models
- Copyright Protection of LLMs for Smart Systems
- Embodied AI Safety and LLM-enabled Cyber-Physical System Safety
- Standardization of AI Accountability in Smart Infrastructures

Submission Guidelines:

Format: All submissions should be written in English with a maximum length of 6 single-spaced, double-column pages using 10pt fonts on 8.5 in x 11 in paper, including all figures, tables, and references, in PDF format. Authors must use the Manuscript Templates for IEEE Conference Proceedings.

Blind Review: Reviewing will be single-blind, i.e., authors can keep their names on their submitted workshop paper.

Submission Portal: **https://edas.info/N33357**

Authors are invited to submit original, unpublished workshop papers that are not currently under review elsewhere. Accepted workshop papers will be included in the conference proceeding published in the IEEE Xplore Digital Library. For all workshop papers, IEEE reserves the right to exclude the workshop paper from distribution after the conference if the workshop paper is not presented at the conference.

Important Dates:

- **Workshop Paper Submission Deadline:** Monday, June 30, 2025
- **Paper Acceptance Notification:** Friday, July 31, 2025

- **Camera-ready Version:** Friday, August 7, 2025
- **Conference Dates:** October 6-8, 2025

10. Promotion Plan

- Co-market with IEEE S&P, USENIX Security, and AAAI conferences
- Partner with ACM SIGSAC and IEEE CIS Cybersecurity communities
- Social media campaign targeting AI security researchers
- Invite authors of recent top papers