AICompS 2025

The International Conference on Artificial Intelligence Computing and Systems

November 26 - 28, 2025
Fukuoka, Japan & Hybrid

Program

ID: 2025111402 — Last updated: Nov 14, 2025

Date	Time	Room A (Track A)	Session Chair	Room B (Track B)	Session Chair
Nov 26	13:00–15:00	**Preparing / Registration**			
	15:00–18:30	**Opening Remarks, Poster Session and Reception** 15:00--16:00: Poster Stage Presentation (3 min. each) 16:00--16:30: Break 16:30--18:30: Presentation in front of the posters & Reception			Kouichi Sakurai (Kyushu Univ.) Chansu Han (NICT)
Nov 27	10:00–11:20	**S1. LLM Evaluation & Reliability** • Not Just Accuracy: Consistency and Reliability as Core Factors in LLM Evaluation • MiniSketch-VQA: A Benchmark for Evaluating LLM-as-a-Judge in Sketch-based Visual Question Answering • The Dual-Edged Sword of Instruction Tuning: An Empirical Study on Precision Gains and Catastrophic Failures • Evaluating Emoji Sequence Generation in Small Language Models	Jihie Kim (Dongguk Univ.)	**S2. Prompt Safety & Grounding** • Vague2Detect: Handling Ambiguous Prompts in Knowledge-Based Open-World Detection • PRISM: Prompt Risk Scoring via Interpretable Semantic Mapping for NSFW Defense • Strong Detection, Short Text: A Four-Class Framework for Human-AI Authorship • Empowering LLM-based Malware Analysis with Synthetic Code	Tao Ban (NICT) Taekyoung Kwon (SNU)
	11:30–13:00	Lunch			
	13:00~13:50	**Keynote I** **"Hyperscale Bug Finding and Fixing: DAPRA AIxCC and Team Atlanta"** Taesoo Kim, Professor, Georgia Tech Team Atlanta placed 1st in the DARPA AI Cyber Challenge (AIxCC), earning a $4M grand prize in the final round. In this talk, I will introduce the DARPA AIxCC competition and share our technical approaches that led to victory—specifically, how we augmented large language models (LLMs) with traditional software analysis techniques to automatically discover and repair security vulnerabilities in real-world, large-scale open-source projects.			Brent ByungHoon Kang (KAIST)
	13:50~14:10	Coffee Break			
	14:10–15:10	**S3. Privacy in Federated / On-Device ML** • Mitigating Label Inference Attacks in Vertical Federated Split Learning through Training Control and Gradient Disturbance • Data Reconstruction Attacks against Privacy Preserving Vertical Federated Learning • ARS-FL-IDS: Accountable Anonymous Federated Learning Against Malicious Behavior	Akira Otsuka (IISEC), Tao Ban (NICT)	**S4. Crypto, FHE & Secure Computation** • An Intra-ciphertext Optimization for Efficient Multi-device Bootstrapping for HE-DNNs • Efficient Evaluation of Indicator Function with Fully Homomorphic Encryption for Privacy-Preserving Embedding • Efficient Batch Verifications for KZG Commitments	Yang Li (UEC)
	15:10~15:40	Coffee Break			
	15:40–17:00	**S5. Medical & Multimodal AI** • Advancing Prehypertension Screening with Explainable AI and Generative Augmentation • Multimodal Pain Intensity Assessment from Physiological Signals: Window Segmentation with Cross-Attention and Temporal Modeling • Multi-Resolution Speckle Priors for Scale-Aware Digital Image Correlation • Enhanced Carbon Emission Prediction in IoT using Optimized Rotation-Invariant Coordinate Convolutional Neural Network for Accurate Urban Environmental Monitoring	Jonghyun Choi (SNU)	**S6. Blockchain Systems & Data Infrastructure** • Mitigating Data Poisoning Attack in On-Device Learning Anomaly Detectors via Peer Consensus • Blockchain-Based Smart Contract Revocable Bidding Scheme for European Union Emissions Trading Scheme • Performance Bottleneck Analysis and Technical Debt in a Non-Standard Hyperledger Fabric CLI Gateway Architecture • Blockchain-Assisted Resource Scheduling for SB-SPS in V2X Networks • Service-aware Resource Management in Cloud computing for HPC workload	Akira Otsuka (IISEC)
	18:00–21:00	**Banquet** @ Sanshiro			
Nov 28	09:30–10:50	**S7. Systems for Efficient AI & Real-Time** • Calypso: A Compiler-Runtime Framework for Configurable Kernel Support in CXL-PNM • Grasle: Graph-level Scheduling Language and Framework for Deep Neural Network • Design and Implementation of a Timing Monitoring System for Real-Time Assurance based on AUTOSAR Timing Protection • Accelerating ONNX Runtime Inference Through Tiling and IO-Binding based Model Design	Tao Ban (NICT)	**S8. Applied AI for Civic & Public Safety** • Spatial-Temporal Graph Neural Networks for Non-Emergency Reports: A Case Study • Context-Aware Safety Report Classification via Large Language Models and Dynamic Knowledge Graphs • HieraText: Unsupervised Multi-Label Hierarchical Text Classification through Adaptive Clustering • Web-Search-Integrated RAG for Resource-Constrained Environments: A Small-Model Approach	Sooel Son (KAIST)
	10:50–11:20	Coffee Break			
	11:20–12:20	**S9. LLM Security & Evaluation at Scale** • The Survey of Jailbreak Attacks on Large Language Models and Defenses • OpenScore: An Agent-Based Framework for Automated Evaluation of AI Model Transparency • BaSTion: Backdoor Style Trigger Identification Method via GANs and Style Transfer Networks	Daehee Jang (Kyunghee Univ.) Hyoungshick Kim (Sungkyunkwan Univ.)	**S10. Attacks & Systems Security** • H-IDE: Hardware Interleaving for Deterministic Encryption to Mitigate Ciphertext Side-Channel Attacks • Model Extraction Attack Leveraging Fractal Images on Color Image Classification Tasks • Applying AI Modeling Attacks as Assessment Tool for Analog PUF-Based Authentication Protocol Evaluation	Tao Ban (NICT)
	12:20–14:00	Lunch			
	14:00–14:50	**Keynote II** **"Navigating the AI Revolution: Ensuring Security and Safety of Frontier AI"** LAM Kwok Yan, Professor of Computer Science, College of Computing and Data Science, Nanyang Technological Universit, Singapore As artificial intelligence evolves from traditional machine learning to foundation models and agentic AI, society stands at a widening frontier of both opportunity and risk. This talk will examine how accelerating capabilities, emerging autonomy, and deepening societal integration have transformed AI safety and security from isolated technical issues into systemic and socio-economic priorities. It will discuss the expanding AI attack surface across data, models, and deployment pipelines, highlighting the risk of Gen AI being misused by cyber-attackers to cyber offences. This talk will also discuss defensive approaches in response to AI risks test and evaluation, red-teaming, interpretability, monitoring etc that form the backbone of trusted AI operations. Looking ahead, it will discuss risks due to the rise of agentic AI, autonomous systems capable of goal-directed behaviour and self-adaptation and the safety and security challenges this poses.			Kouichi Sakurai (Kyushu Univ.)
	14:50–15:25	Coffee Break			
	15:25–16:35	**S11. Secure AI Supply Chain & Transparency** • Fine-Tuning Large Language Models for Malicious Package Detection • Automated Vulnerability Repair based on Language Agent Tree Search • MaquillAI: Generative AI for Personalized Makeup Tutorial • Variables for Free: Breaking MAYO via Valid Solutions	Daehee Jang (Kyunghee Univ.)	**S12. FinTech / Crypto Analytics** • CollaG: Secure and Efficient Collaborative Cloud-Assisted Garbled Circuits • Hybrid GCN–GRU Model for Anomaly Detection in Cryptocurrency Transactions • Hall Sensor-based Ellipse Fitting for Non-Contact Ball Joint Position Estimation • Design and Implementation of KI Cloud R&D Platform for HPC Workloads	Jiwon Seo (SNU)
	16:35–17:15	**Best Paper Awards**			Kouichi Sakurai (Kyushu Unive., Brent Kang (KAIST)
	17:15–17:45	**Closing Remarks**			

Keynote (50 min. / presentation), Full Paper (20 min. / presentation), Short Paper (15 min. / presentation)