AICompS 2025

The International Conference on Artificial Intelligence Computing and Systems

November 26 - 28, 2025
Fukuoka, Japan & Hybrid

Program

ID: 2025112401 — Last updated: Nov 24, 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 (greeting from the president of KIPS, etc.), Poster Session and Reception** 15:00--16:00: Poster Stage Presentation (3 min. each) Po-01 Security-Native Context Awareness Based Zero Trust Architecture for Digital Identity and Sovereignty Po-02 A Three-Layer Network Content Protection Architecture based on LLM Technologies Po-03 From Fatigue to Action: Revisiting AI-Driven SIEM for Effective Incident Response Po-04 AI Security Portal Facilitating Knowledge Consolidation to Promote AI Security Po-05 CTI Technique Extraction Aligned to MITRE ATT&CK via Ensemble LLMs Po-06 A Deployable, End-to-End Framework for Explainable and Federated Phishing Detection in Low-Resource Languages Po-07 ME-XHRL: Malware Evasion using Explainable Hierarchical Reinforcement Learning Po-08 Quantum AI-Driven Anomaly Detection for 6G Network Security Po-09 Signal Fingerprinting Method Based on Emphasized Spectrum Data for Bluetooth Low Energy Po-10 A Two-Stage Legal Document Automation System Combining Template Mapping and LLM-based Post-processing Po-11 Deposit Go : A Conversational AI for Legal Document Generation using LangChain and LangGraph Po-12 Comparison of LLMs: Evaluating Their Abilities of Identifying the Source of Information 16:00--16:30: Break 16:30--18:30: Presentation in front of the posters & Reception		Po-13 AI and Machine Learning Approaches for Early Stroke Detection via Facial and Speech Analysis Po-14 Strain Estimation in Real Tensile Experiments Using Self-Supervised Learning-Based Digital Image Correlation (DIC) Po-15 CAPTION-GUIDED REFINEMENT OF IMAGE REGIONS VIA MASKED GAN TRAINING Po-16 Enhancing Time-Series Predictions through Social Feature Integration: An Empirical Study with RNN and Encoder-Decoder Models Po-17 Unified Fuzzy Framework for Feature Selection and Channel-wise Rule-based Classification in Deep–Fuzzy Hybrid Models Po-18 Advanced Pioneer Algorithm: Inheritance-Based Pioneer-Inspired Optimization Algorithm Po-19 PLC Meets RISC-V: A Trusted Execution Environment Framework for Secure Automation with Multi-Enclave Capability Po-20 FoTo: Targeted Visual Topic Modeling for Focused Analysis of Short Texts Po-21 Hybrid GCN-GRU Model for Anomaly Detection in Cryptocurrency Transactions	Kouichi Sakurai (Kyushu Univ.) Chansu Han (NICT)
Nov 27	10:00–11:20	**S1. LLM Evaluation & Reliability** Pr-01 Not Just Accuracy: Consistency and Reliability as Core Factors in LLM Evaluation Pr-03 MiniSketch-VQA: A Benchmark for Evaluating LLM-as-a-Judge in Sketch-based Visual Question Answering Pr-05 The Dual-Edged Sword of Instruction Tuning: An Empirical Study on Precision Gains and Catastrophic Failures Ps-01 Evaluating Emoji Sequence Generation in Small Language Models	Jihie Kim (Dongguk Univ.)	**S2. Prompt Safety & Grounding** Pr-02 Vague2Detect: Handling Ambiguous Prompts in Knowledge-Based Open-World Detection Pr-04 PRISM: Prompt Risk Scoring via Interpretable Semantic Mapping for NSFW Defense Pr-06 Strong Detection, Short Text: A Four-Class Framework for Human-AI Authorship Ps-02 Empowering LLM-based Malware Analysis with Synthetic Code	Tao Ban (NICT) Ted 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			
	14:10–15:20	**S3. Privacy in Federated / On-Device ML** Pr-07 Mitigating Label Inference Attacks in Vertical Federated Split Learning through Training Control and Gradient Disturbance Pr-09 Data Reconstruction Attacks against Privacy Preserving Vertical Federated Learning Pr-11 ARS-FL-IDS: Accountable Anonymous Federated Learning Against Malicious Behavior	Akira Otsuka (IISEC), Tao Ban (NICT)	**S4. Crypto, FHE & Secure Computation** Pr-08 An Intra-ciphertext Optimization for Efficient Multi-device Bootstrapping for HE-DNNs Pr-10 Efficient Evaluation of Indicator Function with Fully Homomorphic Encryption forPrivacy-Preserving Embedding Ps-03 Efficient Batch Verifications for KZG Commitments Ps-11 Hall Sensor-based Ellipse Fitting for Non-Contact Ball Joint Position Estimation	Yang Li (UEC)
	15:20~15:40	Coffee Break			
	15:40–17:00	**S5. Medical & Multimodal AI** Pr-12 Advancing Prehypertension Screening with Explainable AI and Generative Augmentation Pr-14 Multimodal Pain Intensity Assessment from Physiological Signals: Window Segmentation with Cross-Attention and Temporal Modeling Pr-15 Multi-Resolution Speckle Priors for Scale-Aware Digital Image Correlation Pr-16 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** Pr-13 Mitigating Data Poisoning Attack in On-Device Learning Anomaly Detectors via Peer Consensus Ps-04 Blockchain-Based Smart Contract Revocable Bidding Scheme for European Union Emissions Trading Scheme Ps-05 Performance Bottleneck Analysis and Technical Debt in a Non-Standard Hyperledger Fabric CLI Gateway Architecture Ps-06 Blockchain-Assisted Resource Scheduling for SB-SPS in V2X Networks Ps-07 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** Pr-17 Calypso: A Compiler-Runtime Framework for Configurable Kernel Support in CXL-PNM Pr-18 Grasle: Graph-level Scheduling Language and Framework for Deep Neural Network Pr-20 Design and Implementation of a Timing Monitoring System for Real-Time Assurance based on AUTOSAR Timing Protection Ps-09 Accelerating ONNX Runtime Inference Through Tiling and IO-Binding based Model Design	Tao Ban (NICT)	**S8. Applied AI for Civic & Public Safety** Ps-08 Spatial-Temporal Graph Neural Networks for Non-Emergency Reports: A Case Study Pr-19 Context-Aware Safety Report Classification via Large Language Models and Dynamic Knowledge Graphs Pr-21 HieraText: Unsupervised Multi-Label Hierarchical Text Classification through Adaptive Clustering Pr-22 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** Pr-23 The Survey of Jailbreak Attacks on Large Language Models and Defenses Pr-25 OpenScore: An Agent-Based Framework for Automated Evaluation of AI Model Transparency Pr-27 BaSTion: Backdoor Style Trigger Identification Method via GANs and Style Transfer Networks	Daehee Jang (Kyunghee Univ.) Hyoungshick Kim (Sungkyunkwan Univ.)	**S10. Attacks & Systems Security** Pr-24 H-IDE: Hardware Interleaving for Deterministic Encryption to Mitigate Ciphertext Side-Channel Attacks Pr-26 Model Extraction Attack Leveraging Fractal Images on Color Image Classification Tasks Pr-28 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			
	15:25–16:15	**S11. Secure AI Supply Chain & Transparency** Pr-29 Fine-Tuning Large Language Models for Malicious Package Detection Pr-31 Automated Vulnerability Repair based on Language Agent Tree Search Ps-12 Variables for Free: Breaking MAYO via Valid Solutions	Daehee Jang (Kyunghee Univ.)	**S12. FinTech / Crypto Analytics** Pr-30 CollaG: Secure and Efficient Collaborative Cloud-Assisted Garbled Circuits Pr-32 Hybrid GCN–GRU Model for Anomaly Detection in Cryptocurrency Transactions	Jiwon Seo (SNU)
	16:15–16:45	**Best Paper Awards**			Kouichi Sakurai (Kyushu Unive., Brent Kang (KAIST)
	16:45–17:15	**Closing Remarks**			

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

Organizer

Supporters