IEEE 2025 CIC/COGMI/TPS JOINT CONFERENCES

CONFERENCE PROGRAM

Pittsburgh, PA, USA
Nov. 11-14, 2025

VERSION
Sept 21

Useful Resources

Conference Website

- CIC: http://www.sis.pitt.edu/lersais/conference/cic/2025
- TPS: http://www.sis.pitt.edu/lersais/conference/tps/2025
- CogMI: http://www.sis.pitt.edu/lersais/conference/cogmi/2025/

all schedules are in ***US EST, GMT-5***

Overview: Nov 11, 2025

Workshops Program: TBA

all schedules are in ***US EST, GMT-5***

Overview Conference Day 1: November 12, 2025

7:15 AM - 8:30 AM	Registration (Room: King's Garden Foyer) and Continental Breakfast (King's Garden 2)		
8:30 AM - 8:45 AM	**Welcome and Opening Remarks** (Steering Committee Chair and Organizing Committee Chairs) (Room: King' Garden 5)		
08:45 AM – 9:45 AM	**Keynote 1** (Room: King' Garden 5) **Norman Sadeh,** Professor, Carnegie Mellon University, USA **Title: Usable Privacy and Security in the Age of AI and the Internet of Things - A Multi-Disciplinary Perspective** (Chair: James Joshi, University of Pittsburgh, USA)		
9:45 AM – 10:00 AM	**Coffee Break** (King' Garden 5)		
10:00 AM – 12:00 AM	**TPS Research Session 1: Security & Privacy in Distributed Learning** (Room: King' Garden 5) Session Chair:	**CIC Research Session 1: Intelligent Learning for Data Systems:** **(Room: King' Garden 2)** Session Chair:	**CIC Research Session 1: Intelligent Learning for Data Systems** (Room: King' Garden 3) Session Chair:
12:00 PM – 01:00 PM	**Lunch Break** (provided by conference) Room: King's Garden 4		
01:00 PM – 02:00 PM	**Keynote 2** (Room: King' Garden 5) **Ece Kamar, CVP and Managing Director, AI Frontiers, Microsoft Research, USA and Affiliated Faculty, University of Washington, USA** **Title: AI Agents as the Next Frontier in AI** (Chair: TBA)		
02:00 PM – 3:30 PM	**Panel 1** (Room: King' Garden 5) **Panel Title: IEEE TPS Panel: Towards building Trustworthy and Responsible Agentic AI** **Panelists**: Elisa Bertino,Professor (Purdue University, USA), Elena Ferrari, Professor (University of Insubria, Italy) and Ling Liu, Professor (Georgia Institute of Technology, USA) **Moderator:** James Joshi, University of Pittsburgh, USA		
03:30 PM – 03:45 PM	**Coffee Break** (King' Garden 5)		
03:45 PM – 05:45 PM	**TPS Research Session 2: Attacks and Defenses on AI Models** (Room: King' Garden 5) Session Chair:)	**CogMI Research Session 2: AI Privacy, Security & Robustness** (Room: King' Garden 2) Session Chair:	**Invited Research/Vision Session 1:** (Room: King' Garden 3) Session Chair:
06:00 PM – 08/09:00 PM	**Networking/Reception** (provided by conference): Room: King's Garden Foyer		

all schedules are in ***US EST, GMT-5***

Overview Conference Day 2: November 13, 2025

7:15 AM - 8:30 AM	Registration (Room: King's Garden Foyer) and Continental Breakfast (King's Garden 2)		
8:30 AM - 8:45 AM	**Welcome and Opening Remarks** (Steering Committee Chair and Organizing Committee Chairs) (Room: King' Garden 5)		
08:45 AM – 9:45 AM	**Keynote 3** (Room: King' Garden 5) **Huan Liu, Regents Professor, Arizona States University, USA** **Title: Ceaseless Inquiries - Lesson Learned from Social Media Mining** (Chair: *)*		
9:45 AM – 10:00 AM	**Coffee Break** (King' Garden 5)		
10:00 AM – 12:00 AM	**TPS Research Session 3: Generative AI, Risks, Attacks, and Defenses** (Room: King' Garden 5) Session Chair:	**CogMI Research Session 3: AI for Human Wellbeing, Education & Healthcare** (Room: King' Garden 2) Session Chair:	**Invited Research/Vision Session 2:** (Room: King' Garden 3) Session Chair:
12:00 PM – 01:00 PM	**Lunch Break** (provided by conference) Room: King's Garden 4		
01:00 PM – 02:00 PM	**Keynote 4** (Room: King' Garden 5) **Dimitrios Gerogakopolous, Director, ARC Industrial Trasformation Research Hub for Future Digital Manufacturing, Australia and Professor, Swinburne University, Australia** **Title: From a digital manufacturing vision to improving industrial productivity and resilience via digital twins, dependency-aware AI, and co-creation with the industry.** (Chair: TBA)		
02:00 PM – 3:30 PM	**Panel 2** (Room: King' Garden 5) **Panel Title: IEEE CogMI Panel: From LLMs and Agentic AI to Artificial General Intelligence (AGI) to Artificial Superintelligence (ASI) – the Paths, The Prospects, and the Pitfalls** **Panelists**: Vincent Conitzer, Professor (Carnegie Mellon University, USA), Sandeep Gopisetty,Director & Distinguished Engineer Enterprise Data & Governance for AI Models (IBM Research - Almaden San Jose, USA) and Huan Liu, Regents Professor (Arizona States University, USA) **Moderator:** *TBA*		
03:30 PM – 03:45 PM	**Coffee Break** (Room: King' Garden 5)		
03:45 PM – 05:45 PM	**TPS Research Session 4: Emerging Frontiers in Security and Trust** (Room: King' Garden 5) Session Chair:	**CogMI Research Session 4: Applied AI, Multimodality & Emerging Paradigms** (Room: King' Garden 2) Session Chair:	**Invited Research/Vision Session 3:** (Room: King' Garden 3) Session Chair:
06:00 PM – 08/09:00 PM	**Banquet** (provided by conference) Room: King's Garden 4		

all schedules are in ***US EST, GMT-5***

Overview Conference Day 3: November 14, 2025

7:15 AM - 8:30 AM	Registration (Room: King's Garden Foyer) and Continental Breakfast (King's Garden 2)		
8:30 AM - 8:45 AM	**Welcome and Opening Remarks** (Steering Committee Chair and Organizing Committee Chairs) (Room: King's garden 5)		
08:45 AM – 9:45 AM	**Keynote 5** (Room: King's garden 5) **Bhavani Thuraisingham, Founders Chair Professor, University of Texas at Dallas, USA** **Title: Artificial Intelligence for Transportation Systems Security and Resiliency** **Chair:** TBA		
9:45 AM – 10:00 AM	Coffee Break (King' Garden 5)		
10:00 AM – 12:00 AM	**TPS Research/Application Session 5: Privacy and Trust in AI & Collaborative Learning** (Room: King' Garden 5) Session Chair:	**CogMI Research/Application Session 5: Applied AI for Systems, Security & Automation** (Room: King's garden 2) Session Chair:	**Invited Research/Vision Session 4:** (Room: King' Garden 3) Session Chair:
12:00 PM – 01:00 PM	**Lunch Break** (provided by conference) **Room**: King's Garden 4		
01:00 PM – 02:00 PM	**Keynote 6** (Room: King's garden 5) **Sergei Vassilvitskii, Distinguished Scientist & Senior Research Director, Google (New York), USA** **Title: Practical Considerations for Differential Privacy and what it means for LLMs** (Chair: TBA)		
02:00 PM – 3:30 PM	**Panel 3** (Room: King's garden 5) **Panel Title: TBA** **Panelists**: Dimitrios Georgakopoulos, Director, ARC Industrial Trasformation Research Hub for Future Digital Manufacturing, Australia and Professor (Swinburne University, Australia), Mahadev Satyanarayanan, Carnegie Group Professor of Computer Science (Carnegie Mellon University, USA) and Bhavani Thuraisingham, Founders Chair Professor (University of Texas at Dallas, USA) **Moderator:** *TBA*		
03:30 PM – 03:45 PM	**Coffee Break (**King' Garden 5)		
03:45 PM – 05:45 PM	**TPS Application Session 6: Vulnerability Detection and Security Defense Mechanisms** (Room: King' Garden 5) Session Chair:	**CogMI Application/Research Session 6: Cognitive Intelligence, Quantum & Scientific Applications** (Room: King's garden 2) Session Chair:	**CIC Research/Application Session 2: Securing AI, Data, and Systems** (Room: King' Garden 3) Session Chair:
06:00 PM – 08/09:00 PM	**Closing remarks** (King' Garden 5)		

IEEE 2024 CIC/CogMI/TPS Joint Conferences
Conference Day 1: November 12, 2025

Registration & Continental Breakfast (provided by conference)

7:15 AM - 8:30 AM

Welcome and Opening Remarks

8:30 am – 8:45 am
All Participants and Chairs
Room - King' Garden 5

Keynote 1 (Room: King' Garden 5)

08:45 AM – 9:45 AM
Norman Sadeh, Professor, Carnegie Mellon University, USA
Title: Usable Privacy and Security in the Age of AI and the Internet of Things - A Multi-Disciplinary Perspective
Session Chair: James Joshi, University of Pittsburgh, USA

Coffee Break (15 min)

TPS Research Session 1: Security and Privacy in Distributed Learning

11:00 am – 12:00 noon
Room: King' Garden 5
Session Chair:

Enabling Privacy-preserving Model Evaluation in Federated Learning via Fully Homomorphic Encryption
Cem Ata Baykara (University of Tübingen), Ali Burak Ünal (University of Tübingen), and Mete Akgün (University of Tübingen)

HERL: Tiered Federated Learning with Adaptive Homomorphic Encryption using Reinforcement Learning
Jiaxiang Tang (University of Minnesota), Zeshan Fayyaz (University of Waterloo), Mohammad Salahuddin (University of Waterloo), Raouf Boutaba (University of Waterloo), Zhi-Li Zhang (University of Minnesota), and Ali Anwar (University of Minnesota)

PPFL-RDSN: Privacy-Preserving Federated Learning-based Residual Dense Spatial Networks for Encrypted Lossy Image Reconstruction
Peilin He (University of Pittsburgh), James Joshi (University of Pittsburgh)

One-Shot Secure Aggregation: A Hybrid Cryptographic Protocol for Private Federated Learning in IoT
Imraul Emmaka (University of Arkansas at Little Rock), Tran Viet Xuan Phuong (University of Arkansas at Little Rock)

RBBD: A Representation-Based Framework for Edge-Case Backdoor Defense in Federated Learning
Samir Poudel (Middle Tennessee State University), Kritagya Upadhyay (Middle Tennessee State University), and Jiblal Upadhyay (Middle Tennessee State University)

Enhancing Resilience in Industrial Control Systems: Rapid Attack Detection, Recovery, and Monotonicity Preservation through STL-GT Online Monitoring
Chidi Agbo (University of Nebraska at Kearney), Hoda Mehrpouyan (Boise State University)

CIC Research Session 1: Intelligent Learning for Data Systems

Time: 10am -12noon
Room: King' Garden 3
Session Chair: TBA

QLPMR: Q-Learning-Based Path Dynamics-Driven Multipath Flow Routing in Software-Defined Vehicular Networking
Patikiri Arachchige Don Shehan Nilmantha Wijesekara (University of Ruhuna), Kalupahana Liyanage Kushan Sudheera (University of Ruhuna), Harsha Sandaruwan Gardiyawasam Pussewalage (University of Agder), Geeth Priyankara Wijesiri (University of Ruhuna) and Peter Han Joo Chong (Auckland University of Technology)

Multi-Strategy Fused Transformer-CNN with PSO-Driven Optimization for Soil Properties Estimation from Hyperspectral Data
Abhyudya Sangwan (Delhi Technological University), Divyashikha Sethia (Delhi Technological University) and Shagun Jain (Delhi Technological University)

An Interpretable and Efficient Random Undersampling-enhanced SHAP Framework for Medicare Fraud Detection
Qianxin Liang (Florida Atlantic University), Richard Bauder (Florida Atlantic University) and Taghi Khoshgoftaar (Florida Atlantic University)

Maximizing Information in Domain-Invariant Representation Improves Transfer Learning
Adrian Shuai Li (Purdue University), Elisa Bertino (Purdue University), Xuan-Hong Dang (IBM T.J. Watson Research Center), Ankush Singla (Purdue University), Yuhai Tu (IBM T.J. Watson Research Center) and Mark N Wegman (IBM T.J. Watson Research Center)

A Digital Twin-Based Approach with a System-Agnostic Integration Method to Enable Intelligence Capabilities and What-If Scenario Orchestration
Abdelhadi Belfadel (IRT SYSTEMX), Stephen Creff (IRT SYSTEMX), Jean-Patrick Brunet (IRT SYSTEMX), Sin-Seok Seo (Safran), Guillaume Doquet (Safran), Kevin Mantissa (IRT SYSTEMX), Christophe Duhil (Cervval), Yann Bouju (Naval Group), Fikri Hafid (RTE) and Amira Ben Hamida (IRT SYSTEMX)

Towards Collaboration-Aware Resource Sharing in Research Computing Infrastructures
Souradip Nath (Arizona State University), Ananta Soneji (Arizona State University), Jaejong Baek (Arizona State University), Carlos Rubio Medrano (Texas A&M University - Corpus Christi) and Gail-Joon Ahn (Arizona State University)

CogMI Research Session 1: Reasoning, Agents & Reinforcement Learning

Time: 10:00am – 12noon
Room: King's garden 2
Session Chair: TBA

Knowledge-guided Continual Learning for Behavioral Analytics Systems
(Yasas Senarath and Hemant Purohit)

An Iterative Multi-Agent Analysis for Automated Evaluation in NLG Tasks
(Hadel Alhawasi, Ruocheng Shan and Abdou Youssef)

Next-Gen Theorem Proving: A Multi-Agent Paradigm for Automated Reasoning
(Akhil Gupta Chigullapally, Ram Dantu, Shakila Zaman and Apurba Pokharel)

Assessing LLM Reasoning with Subtask Variation: Chess and DREAMS
(Carlos Olea, Allen Karns and Jules White)

Object Empowerment-Driven Tool Selection in Reinforcement Learning
(Faizan Rasheed, Daniel Polani, Kenzo Clauw and Nicola Catenacci Volpi)

Online Decision Mamba
(Trenton Ruf and Banafsheh Rekabdar)

Lunch Break

12:00 PM – 1:00 PM

Keynote 2 (Room: King' Garden 5)

01:00 PM – 02:00 PM
Ece Kamar, CVP and Managing Director, AI Frontiers, Microsoft Research, USA and Affiliated Faculty, University of Washington, USA
Title: AI Agents as the Next Frontier in AI
Session Chair: TBA

Panel Session (Room: King' Garden 5)

02:00 PM – 03:30 PM
Panel Title: IEEE TPS Panel: Towards building Trustworthy and Responsible Agentic AI
Panelists: Elisa Bertino,Professor (Purdue University, USA), Elena Ferrari, Professor (University of Insubria, Italy) and Ling Liu, Professor (Georgia Institute of Technology, USA)
Moderator: James Joshi, University of Pittsburgh, USA

Coffee Break (15 min)

TPS Research Session 2: Attacks and Defenses on AI Models

Time: 3:45pm – 5:45pm
Room: King' Garden 5
Session Chair:

Robust Physically Realizable Backdoor Attack
Md Jahirul Islam (Central Queensland University), Kazi Aminul Islam (Kennesaw State University)

Fidelity-Optimizing Defense Mechanism Against Membership Inference Attacks
Md Faisal Ahmed (BRAC University), Zhengdao Wang (George Mason University)

NatGVD: Natural Adversarial Example Attack towards Graph-based Vulnerability Detection
Avilash Rath (University of Texas at Dallas), Weiliang Qi (University of Texas at Dallas), Youpeng Li (University of Texas at Dallas), and Xinda Wang (University of Texas at Dallas)

Explainable but Vulnerable: Adversarial Attacks on XAI Explanation in Cybersecurity Applications
Maraz Mia (Tennessee Technological University), and Mir Mehedi Ahsan Pritom (Tennessee Technological University)

Anomaly Detection in Graphs via Topology-Aware Attention Mechanisms
Narges Alipourjeddi (Toronto Metropolitan University) and Ali Miri (Toronto Metropolitan University)

It's about time!: Exploiting Timing Variance for IoT Device-type Fingerprinting
Maxwel Bar-On, Alanood Alqobaisi (Colorado State University), Bruhadeshwar Bezawada (Southern Arkansas University), Indrakshi Ray (Colorado State University), and Indrajit Ray (Colorado State University)

Invited Session 1:

Time: 3:45pm – 5:45pm
Room: King' Garden 3
Session Chair: TBA

CogMI Research Session 2: AI Privacy, Security & Robustness

Time: 3:45pm – 5:45pm
Room: King's garden 2
Session Chair: TBA

Evaluating Human and Machine Confidence in Phishing Email Detection: A Comparative Study
(Paras Jain, Khushi Dhar, Olyemi E. Amujo and Esa M. Rantanen)

Restricted Hopfield Networks are Resilient to Adversarial Perturbations
(Ci Lin, Tet Yeap, Iluju Kiringa and Biwei Zhang)

Edge-Optimized Privacy: Synthetic Data Generation Using Hybrid SMOTE & Autoencoder
(Kiana Katouzian and Ahmad Patooghy)

RL-MoE: An Image-Based Privacy Preserving Approach In Intelligent Transportation System
(Abdolazim Rezaei, Mehdi Sookhak and Mahboobeh Haghparast)

Deep Metric Stylometry: Learning Author Signatures from Style and Semantics
(Mostafa Rahgouy, Mehnaz Tabassum, Amit Das, Dongji Feng, Gerry Dozier and Cheryl D. Seals)

Breaking the Chain: A Systematic Study of Retrieval Failures and LLM Hallucinations in RAG Systems (Application Track)
(Sachintha Kodikara)

Emergent Biases in Large Language Models: A Critical Review of Taxonomy and Evaluations (Application-Track)
(Shawn Ismail and Ramazan Aygun)

Networking/Reception (provided by the conference)
06:00 PM – 09:00 PM

IEEE 2024 CIC/CogMI/TPS Joint Conferences
Conference Day 2: November 13, 2025

Registration & Continental Breakfast (provided by conference)

7:15 AM - 8:30 AM

Welcome and Opening Remarks

8:30 am – 8:45 am
All Participants and Chairs
Room - King' Garden 5

Keynote 3 (Room: King' Garden 5)

08:45 AM – 9:45 AM
Huan Liu, Regents Professor, Arizona States University, USA
Title: Ceaseless Inquiries - Lesson Learned from Social Media Mining
Session Chair: TBA

Coffee Break (15 min)

TPS Research Session 3: Generative AI, Risks, Attacks, and Defenses

Time: 10:00am – 12noon
Room: **King' Garden 5**
Session Chair:

Data Access Control in Large Language Models
Nouha Oualha (CEA LIST), Christophe Janneteau (CEA LIST)

Clone What You Can't Steal: Black-Box LLM Replication via Logit Leakage and Distillation
Kanchon Gharami (Virginia Tech), Hansaka Aluvihare (Virginia Tech), Shafika Showkat Moni (Virginia Tech), Berker Peköz (Virginia Tech)

PRvL: Quantifying the Capabilities and Risks of Large Language Models for PII Redaction
Leon Garza (The University Of Texas at El Paso), Anantaa Kotal (The University Of Texas at El Paso), Aritran Piplai (The University Of Texas at El Paso), Lavanya Elluri (Texas A&M University-Central Texas), Prajit Kumar Das (Cisco Systems Inc) and Aman Chadha (Amazon Web Services)

LLMalMorph: On the Feasibility of Generating Variant Malware using Large-Language-Models
Md Ajwad Akil (Purdue University), Adrian Shuai Li (Purdue University), Imtiaz Karim (Texas UT Dallas), Arun Iyengar (IBM), Ashish Kundu (Cisco), Vinny Parla (Cisco), Elisa Bertino (Purdue University)

CipherBERT: A Systematic Framework for High-Accuracy Encrypted Transformer Inference
Nisarg Bhavsar (IIT Kharagpur) and Zaid Ahmed Khan (IIT Kharagpur)

CoDICE: Roll the DICE for Firmware Attestation
Rakesh Podder (Colorado State University), Jason Simental, Elmaddin Azizli, Bharadwaj Mantha, and Indrajit Ray (Colorado State University)

CogMI Research Session 3: AI for Human Wellbeing, Education & Healthcare

Time: 10:00am – 12noon
Room: **King's garden 2**
Session Chair: TBA

Effect of Anxiety Reduction Interventions on Exam Anxiety for Engineering Students Using Physiological Signals
(Jyotiska Bharadwaj, Ayushi Dey, Aditya Bibhas Sahu, Karan Maheshwari, Sanat Chaudhury, Divyasikha Sethia and Sonia Baloni Ray)

AI for Supporting Dispatchers' Mental Health: Proof-of-Concept for Stress Detection Based on Emotional State
(Christin Salley, Daehwan Yoo, Michelle Chatell, Sabine Loos, Stacey Hall and Lu Wang)

Dynamic Stress Detection: A Study of Temporal Progression Modelling of Stress in Speech
(Vishakha Lall and Yisi Liu)

Uncertainty-Aware Temporal Modeling for Student Dropout Prediction in Online Learning Environments
(Ikram Gagaoua)

Self-Supervised Learning for MRI Representation and Cross-Domain Classification of Brain Diseases
(Rishab Darshan Shylendra, Pavithran Gnanasekaran, Piyush Gulhane and Alina Vereshchaka)

ELM: Leveraging Large Language Models for Reliable Emotion Recognition
(Richard Feng)

Transfer Learning based Cognitive Load Monitoring from Cognitive Motor Integration (CMI): An ML-IoT Framework
(Sumona Mukhopadhyay, Mahima Chaudhary, Meaghan Adams, Lauren E Sergio and Marin Litoiu)

Invited Session 2:

Time: 10:00am – 12noon
Room: **King' Garden 3**
Session Chair: TBA

Lunch Break

12:00 PM – 1:00 PM

Keynote 4 (Room: King' Garden 5)

01:00 PM – 02:00 PM
Dimitrios Gerogakopolous, Director, ARC Industrial Trasformation Research Hub for Future Digital Manufacturing, Australia and Professor, Swinburne University, Australia
Title: From a digital manufacturing vision to improving industrial productivity and resilience via digital twins, dependency-aware AI, and co-creation with the industry.
Session Chair: TBA

Panel Session (Room: King' Garden 5)

02:00 PM – 03:30 PM
Panel Title: IEEE CogMI Panel: From LLMs and Agentic AI to Artificial General Intelligence (AGI) to Artificial Superintelligence (ASI) – the Paths, The Prospects, and the Pitfalls
Panelists: Vincent Conitzer, Professor (Carnegie Mellon University, USA), Sandeep Gopisetty,Director & Distinguished Engineer Enterprise Data & Governance for AI Models (IBM Research - Almaden San Jose, USA) and Huan Liu, Regents Professor (Arizona States University, USA)
Moderator: TBA

Coffee Break (15 min)

TPS Research Session 4: Emerging Frontiers in Security and Trust

Time: 3:45pm – 5:45pm
Room: **King' Garden 5**
Session Chair:

Limitations of Watermarking AI-Generated Speech using AudioSeal
Shameer Faziludeen (University College Cork), Arun Sankar M. S. (South East Technological University), Phillip DeLeon (University of Colorado Denver), Utz Roedig (University College Cork)

Diffusion Based DeepFake Generation via Image Editing and Image Morphing
Liyue Fan (UNC Charlotte), Joseph Roberson (UNC Charlotte)

EDL: Efficient Data-oblivious Loops
Biniyam Tiruye (University of Michigan), Lauren Biernacki (Lafayette College), Todd Austin (University of Michigan)

Decoding the Decoders: An Empirical Study of Reverse Engineering Questions on Stack Exchange
Md Rakibul Islam (Lamar University), Md Humaun Kabir (Bangamata Sheikh Fojilatunnesa Mujib Science & Technology University), Anwarul Islam Sifat (Jashore University of Science and Technology)

PQC-LEO: An Evaluation Framework for Post-Quantum Cryptographic Algorithms
Callum Turino (Edinburgh Napier University), William J. Buchanan (Edinburgh Napier University), Owen Lo (Edinburgh Napier University), Christoph Thümmler (Edinburgh Napier University)

Explainable AI in Data Poisoning Threat Models Across the CIA Triad: A Smart Grid Case Study
Authors: Gustavo Sanchez (Karlsruhe Institute of Technology), Ghada Elbez (Karlsruhe Institute of Technology) and Veit Hagenmeyer (Karlsruhe Institute of Technology)

CogMI Research Session 4: Applied AI, Multimodality & Emerging Paradigms

Time: 3:45pm – 5:45pm
Room: **King's garden 2**
Session Chair: TBA

Dependence Minimization for Multi-Label Classification: An Alternative to Human Labeling
(Alex Metzger, Ram Dantu, Alexis Blackwell and Thomas McCullough)

SentiGAT: Enhancing Multimodal Sentiment Analysis via Graph Attention Network-Based Feature Fusion and Alignment
(Misbah Ul Hoque and Kisung Lee)

Cross-Country Analysis of Discourse on Misinformation in the Digital Platform Using Topic Modeling
(Minh Nguyen, Kuheli Sai, Deepti Gupta and Quang-Thinh Bui)

Cognitive Data Architecture for Financial Services: A Benchmark-Driven Framework for Real-Time, AI-Enabled Compliance and Risk Management
(Bharat Chaturvedi)

Towards Multimodal Solar Flare Prediction Using Magnetic Polarity Inversion Lines
(Ziba Khani, Reza Mansouri and Berkay Aydin)

Explaining at the Speed of Sight: Attention-Aware XAI for OODA-Inspired AI Design
(Dylan Wright and Vineetha Menon)

ConvFormer: A Strong Convolutional Baseline for Multi-Agent Trajectory Prediction
(Yury Davydov, Wen-Hui Chen and Yu-Chen Lin)

Invited Session 3:

Time: 10:00am – 12noon
Room: **King' Garden 3**
Session Chair: TBA

Banquet Dinner (provided by the conference)

06:00 PM – 09:00 PM

IEEE 2024 CIC/CogMI/TPS Joint Conferences
Conference Day 3: November 14, 2025

Registration & Continental Breakfast (provided by conference)

7:15 AM - 8:30 AM

Welcome and Opening Remarks

8:30 am – 8:45 am
All Participants and Chairs
Room - King' Garden 5

Keynote 5 (Room: King' Garden 5)

08:45 AM – 9:45 AM
Bhavani Thuraisingham, Founders Chair Professor, University of Texas at Dallas, USA
Title: Artificial Intelligence for Transportation Systems Security and Resiliency
Session Chair: TBA

Coffee Break (15 min)

TPS Research/Application Session 5: Privacy and Trust in AI & Collaborative Learning

Time: 10:00am – 12noon
Room: **King' Garden 5**
Session Chair:

A Privacy-Fidelity Tradeoff Framework in Post-Processed Machine Learning
Md Faisal Ahmed (BRAC University), Zhengdao Wang (George Mason University)

Learning from Literature: A Retraining-Free Framework for LLM Jailbreak Defense via NLP-based Adversarial Literature Analysis
Sheikh Samit Muhaimin (University of Notre Dame), Spyridon Mastorakis (University of Notre Dame)

Images in Motion?: A First Look into Video Leakage in Collaborative Deep Learning
Md Fazle Rasul (Colorado State University), Alanood Alqobaisi (Colorado State University), Bruhadeshwar Bezawada (Southern Arkansas University), Indrakshi Ray (Colorado State University)

Privacy-Preserving AI-Enabled Decentralized Learning and Employment Records System
Yuqiao Xu (Case Western Reserve University), Mina Namazi (Case Western Reserve University), Sahith Reddy Jalapally (Case Western Reserve University), Osama Zafar (Case Western Reserve University), Youngjin Yoo (Case Western Reserve University), Erman Ayday (Case Western Reserve University)

FALCON: Federated Anomaly Learning and COllaborative Network for Secure Autonomous Vehicles

Riadh Ben Chaabene (ÉTS Montréal), Darine Ameyed (ÉTS Montréal), Fehmi Jaafar (ÉTS Montréal), Mohamed Cheriet (ÉTS Montréal)

GAKA-D2D: A lightweight Group AKA Scheme for D2D Communication in Emergency Scenarios (Research)
Ponjit Borgohain (Cotton University), Hiten Choudhury (Cotton University)

CogMI Research/Application Session 5: Applied AI for Systems, Security & Automation

Time: 10:00am – 12noon
Room: **King's garden 2**
Session Chair: TBA

Where to Explore: A Reach and Cost-Aware Approach for Unbiased Data Collection in Recommender Systems
(Qiang Chen and Venkatesh Ganapati Hegde)

Hybrid Classical-Quantum Neural Network for Distributed Denial of Service Attacks Detection
(Ahmad Alomari and Sathish Kumar)

Preventing Data Poisoning in Continual Learning for AI Generated Text Detectors
(Ian Miller and Dan Lin)

Human-in-the-Loop Runbook Improvement with Agentic Support Automation
(Rocker D'Antonio and Harry Xie)

MEAT: Mixture of Experts in Action Transformer for Robotic Arm Control (Research)
(Naeem Ul Islam, Hung Mai Phan Quoc and Zheng Yingren)

Dynamic Reward Scaling for Multivariate Time Series Anomaly Detection: A VAE-Enhanced Reinforcement Learning Approach (Application-Track)
(Bahareh Golchin and Banafsheh Rekabdar)

Enabling Lifelong Learning in AI with Biological Neural Networks Based on Short-Term, Working, and Long-Term Memory
(Hanav Modasiya) **(Application-Track)**

Invited Session 4:

Time: 10:00am – 12noon
Room: **King' Garden 3**
Session Chair: TBA

Lunch Break

12:00 PM – 1:00 PM

Keynote 6 (Room: King' Garden 5)

01:00 PM – 02:00 PM
Sergei Vassilvitskii, Distinguished Scientist & Senior Research Director, Google (New York), USA
Title: Practical Considerations for Differential Privacy and what it means for LLMs
Session Chair: TBA

Panel Session (Room: King' Garden 5)

02:00 PM – 03:30 PM
Panel Title: TBA
Panelists: Dimitrios Georgakopoulos, Director, ARC Industrial Transformation Research Hub for Future Digital Manufacturing, Australia and Professor (Swinburne University, Australia), Mahadev Satyanarayanan, Carnegie Group Professor of Computer Science (Carnegie Mellon University, USA) and Bhavani Thuraisingham, Founders Chair Professor (University of Texas at Dallas, USA)
Moderator: TBA

Coffee Break (15 min)

TPS Application Session 6: Vulnerability Detection and Security Defense Mechanisms

Time: 3:45pm – 5:45pm
Room: **King' Garden 5**
Session Chair:

MAVUL: Multi-Agent Vulnerability Detection via Contextual Reasoning and Interactive Refinement
Youpeng Li (University of Texas at Dallas), Kartik Joshi (University of Texas at Dallas), Xinda Wang (University of Texas at Dallas), Eric Wong (University of Texas at Dallas)

Leveraging Transformer Models and eXplainable Reinforcement Learning Methods for Advanced Intrusion Detection and Response System
Mohammad Ghasemigol (Old Dominion University), Daniel Takabi (Old Dominion University)

GPS Spoofing Attacks and Pilot Responses Using a Flight Simulator Environment
Mathilde Durieux (University of Kansas), Kayla Taylor (University of Kansas), Laxima Niure Kandel (University of Kansas), Deepti Gupta (University of Kansas)

VulnDetective: Using LLM Agents to Analyze Common Weaknesses and Identify Smart Contract Vulnerabilities
Thanmai Mandala (University at Buffalo), Cora Zeger (University at Buffalo), Tessa Andersen (University at Buffalo), Gaby G. Dagher (Concordia University), Jun Zhuang (University at Buffalo)

XAST: Explainable AST-Transformer for Smart Contract Vulnerability Detection
Harshith Sai Veeraiah (University of North Texas), Syed Badruddoja (University of North Texas), Ram Dantu (University of North Texas)

Guiding Reinforcement Learning Using Uncertainty-Aware Large Language Models
Maryam Shoaeinaeini (University of Kentucky), Brent Harrison (University of Kentucky)

CIC Research/Application Session 2: Securing AI, Data, and Systems

Time: 3:45 pm – 5:45 pm
Room: **King' Garden 3**
Session Chair: TBA

Shielding Against Deception: Fortifying Deepfake Detectors Against Data Poisoning Attacks
Ian Miller(Vanderbilt University), Chaoquan Cai (Vanderbilt University), Maya Cutkosky (Vanderbilt University) and Dan Lin (Vanderbilt University)

Access Control Policies Specification and Analysis for Multi-Institutional Collaborative Projects
Abhimanyu Chawla (Colorado State University), Mahmoud Abdelgawad (Colorado State University) and Indrakshi Ray (Colorado State University)

ShadowScan: LLM-Based Device Fingerprinting in IoT Networks
Duwarahavidyan Jeganathan (University of Ruhuna), Tharuka Harshajith Bandara (University of Ruhuna), Harsha Sandaruwan Gardiyawasam Pussewalage (University of Agder), Thilina Deshan Dissnayake (University of Ruhuna), Dnithi Sachinthana Fernando (University of Ruhuna), Kushan Sudheera Kalupahana Liyanage (University of Ruhuna) and Thilini Dahanayaka (University of Sydney)

Strategic Incentivization for Locally Differentially Private Federated Learning
Yashwant Krishna Pagoti (IIT Kharagpur), Arunesh Sinha (Rutgers University) and Shamik Sural (IIT Kharagpur)

Blockchain Based Spectrum Leasing for 5G and Beyond
Dilshara Niromali (University of Ruhuna), Sampavi Sivakumaran (University of Ruhuna), Harsha Sandaruwan Gardiyawasam Pussewalage (University of Agder), Sachith Piumantha (University of Ruhuna), Geeth P. Wijesiri (University of Ruhuna) and Indika A. M. Balapuwaduge (University of Agder)

RideCred: A Decentralized and Incentive-Driven Ride-Sharing System with Trustless Coordination
Shailesh Kumar Sharma (IIT Kharagpur), Balaji Palanisamy (University of Pittsburgh), Shamik Sural (IIT Kharagpur) and Sandip Chakraborty (IIT Kharagpur)

CogMI Application/Research Session 6: Cognitive Intelligence, Quantum & Scientific Applications

Time: 3:45pm – 5:45pm
Room: **King's garden 2**
Session Chair: TBA

MORAL: A Multimodal Reinforcement Learning Framework for Cognitive Intelligence in Autonomous Laboratories
(Natalie Tirabassi, Sathish Kumar, Sumit Jha and Arvind Ramanathan)

The Imitation Fallacy: Why Behavioral Equivalence Cannot Verify Artificial Consciousness
(Aayush Gauba)

A novel graph neural network architecture for predicting drug-target interactions
(Brandon Warner, Avi Ruthen, Edward Ratner, Elliot Farmer Garcia and Christopher Douglas)

Quantum Regression for Cognitive Intelligence in Complex Environments
(Ahmad Alomari and Sathish Kumar)

Quantum Clustering for Cognitive Intelligence: Methods, Applications and Challenges (Research)
(Ahmad Alomari and Sathish Kumar)

Robust and Efficient Traffic Monitoring System Under Adverse Weather
(Ramy Othman, Anisha Mulinti, William O'Donnell, Weitian Wang and Michelle Zhu)

Prompts and Thoughts: Can Your Cyber Curriculum Meet the Job Skills
(Alexis Blackwell, Ram Dantu, Alex Metzger and Vinh Quach)

Closing Remarks

5:45pm – 6:15pm
Room: **King' Garden 5**