IEEE 2025 CIC/COGMI/TPS JOINT CONFERENCES

CONFERENCE PROGRAM

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

Useful Resources

Conference Websites

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

Workshops websites (QR Code to Program details)

AIRET

DISTILL

EIC

SPIRIT

QUILLS

CIST

TPHAC

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

Overview: Nov 11, 2025: Workshops Program

Workshop AIRET (**Room**: King's Garden 5)	Workshop SR-CIST (**Room**: King's Garden 3)	Workshop TP-HAC (**Room**: King's Garden 1)	Workshop HMD-SPiRiT (**Room**: Brigade Room)	Workshop QuiLLs (**Room**: King's Garden 2)	Workshop DISTILL (**Room**: Rivers Room)	Workshop EIC (**Room**: King's Plaza)

ROOM ----	**King's Garden 5**	**King's Garden 3**	**King's Garden 1**	**Brigade Room**	**King's Garden 2**	**Rivers Room**	**King's Plaza**
Time	**Workshop AIRET**	**Workshop SR-CIST**	**Workshop TP-HAC**	**Workshop HMD-SPiRiT**	**Workshop QuiLLs**	**Workshop DISTILL**	**Workshop EIC**
7am – 8:30am (Breakfast will be in King Garden 4)	Registration + Breakfast	Registration + Breakfast	Registration + Breakfast	Registration + Breakfast	Registration + Breakfast	Registration + Breakfast	Registration + Breakfast
8:30 am – 8:45 am	Opening	Opening	Opening	Opening	Opening	Opening	Opening
8:45 am -9:45am	Paper presentation: Session 1: Trust, Governance, and Ethics in Multi-Agent AI Systems	Keynote: Dr. Greg Shannon, Idaho National Laboratory Fellow and Chief Cybersecurity Scientist. Talk Title: Foundations for Trust, Privacy, and Security in Proliferated Spaces	Keynote: Jason Hong, CMU | Title: Auditing AI Systems for Bias and Fairness	Papers Session 1: Privacy, and Public and Mobile Health	Keynote 1: Zheshen Zhang, UMich | Title: Quantum Information Processing Enhanced by Entanglement and AI	Paper session 1	Keynote Presentation: Dr. Amina Blackwood-Meeks
9:45am -10:00 am	Coffee Break	Coffee Break	Coffee Break	Coffee Break	Coffee Break	Coffee Break	Coffee Break
10:00 pm– 11:00 pm	Keynote: Vincent Conitzer, CMU | Title: Game Theory for AI Agents	Paper Presentation Session 1	Keynote: Weisong Shi, University of Delaware | Title: Vehicle Computing: A New Computing Paradigm in the Era of Autonomous Driving	Paper Session 2: Cybersecurity, Privacy and/or Resilience in Healthcare data and LLMs	[10:00 am - 12:05pm] Session 1: Entanglement Frontier, Session Chair: Kaushik P. Seshadreesan	10:00 am- Invited Talk: Dr. Benjamin Steenhoek, Microsoft 10:30 am- Invited Talk: Dr. Tunazzina Islam, Purdue University	Working session 1: Beyond Standard English: Jamaican Experiences with Voice-Enabled AI Technologies
11:00 pm – 12:00/15pm	AIRET Panel : The Human Role in Agentic AI Futures	[11am-12:15pm] Panel: Operational Technology (OT) Security	[11am-12:15pm] TPHAC Panel on Trustworthy- and privacy-by-design Human-AI collaboration Systems	[11am-11:15pm] Break [11:15am-12:15pm] Keynote: Brad Malin, Vanderbilt University Title: Building Responsible and Reliable AI-Driven Technologies for Biomedicine		DISTILL Panel: Secure, Trustworthy, and Explainable AI in a Connected World	Working session 2: AI Use by Higher Education Students Leading to Self-Efficacy in Their Classroom Verbal and Written Communication Skills
12:00 pm -1:30 pm (Lunch will be in King Garden 4)	Lunch time window	[12:15pm-1:30pm] Lunch time window	[12:15pm-1:30pm] Lunch time window	[12:15pm-1:30pm] Lunch time window		Lunch time window	Lunch
1:30 pm - 2:30 pm	Paper presentation Session 2: Security, Risk, and Control of Intelligent Agents	Paper presentation session 2	[1:30 - 2:50pm] Paper Session 1: Trust & Human–AI Collaboration	Paper session 3: Medical Devices and Privacy at Scale	Keynote 2: Ashish Kundu, Head of Cybersecurity Research, Cisco Research | Title: Quantum Secure Networks	1:30 pm- Invited Talk: Dr. Imtiaz Karim (UT Dallas) 2:00 pm- Invited Talk: Dr. Farimah Farahmandi (University of Florida)	Working session 3: Understanding the Language Use Differences between Reviews Associated with Star Rated Restaurants on Yelp
2:30 pm - 3:30 pm	Paper presentation Session 3: Human-Centered Design and Optimization	**Invited talk: Sekar Kulandaivel, PhD – Bosch**		[2:30 -3:00pm] Invited Industry Talk: From CVE Alert to Patient Risk - Why Context Matters in Medical Device Security Ken Zalevsky, CEO at Vigilant Ops	Session 2: Algorithm Frontier Session Chair: Junyu Liu	2:30 pm: Invited Talk: Dr. Saikat Chakraborty, Microsoft 3:00 pm: Invited Talk: Dr. Sayem Mohammad Imtiaz, Meta	Working session 4: Towards a Hybrid Human-Machine Framework for Gunshot Identification and Police Notification in Jamaica
			[2:50 - 3:20pm] Coffee Break	[3:00 - 3:15] Coffee			
3:30 pm – 3:45 pm	Coffee	Coffee	[3:20 - 4:40pm] Paper Session 2 Privacy, Security & Human–AI Collaboration	[3:15 - 4:30pm] Panel : Securing the Health Data & Device Lifecycle: Privacy, Resilience, and Trust from Clinic to Cloud [4:30 - 5:00pm] Discussion & Closing	Coffee	Coffee	Coffee
3:45 – 5:00pm	[3:45 - 4:30] Spotlight Talk: Dr. Thanh Tran, Amazon Inc. [4:30 - 5:00] Closing Conversation + Adjournment	[3:45 - 4:45] Paper Presentation Session 3, [4:45 - 5:00] Closing + Adjournment			[3:45 - 4:30] Panel Discussions: Quantum Academia & Industry	Paper session 2 + adjournement	Action Planning & reflection

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 Light Breakfast (King's Garden 4)		
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 1** (Room: King's Garden 5) **Norman Sadeh,** 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's Garden 5)		
10:00 AM – 12:00 AM	**TPS Research Session 1: Security & Privacy in Distributed Learning** (Room: King's Garden 5) Session Chair: Bruhadeshwar Bezawada, Southern Arkansas University (USA)	**CogMI Research Session 1: Intelligent Learning for Data Systems:** **(Room: King's Garden 2)** Session Chair: Reza Zafarani, Syracuse University (USA)	**CIC Research Session 1: Intelligent Learning for Data Systems** (Room: King's Garden 3) Session Chair: Balaji Palanisamy, University of Pittsburgh, USA
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's Garden 5) **Ece Kamar, Microsoft Research, USA and University of Washington, USA** **Title: AI Agents as the Next Frontier in AI** (Chair: Danda B. Rawat, Howard University, USA)		
02:00 PM – 3:30 PM	**Panel 1** (Room: King's Garden 5) **Panel Title: IEEE TPS Panel: Towards building Trustworthy and Responsible Agentic AI** **Panelists**: Elisa Bertino (Purdue University, USA), Matthew Gaston (Carnegie Mellon University Software Engineering Institute, USA), Heiko Ludwig (IBM Research, USA) and Ling Liu (Georgia Institute of Technology, USA) **Moderator:** James Joshi, University of Pittsburgh, USA		
03:30 PM – 03:45 PM	**Coffee Break** (King's Garden 5)		
03:45 PM – 05:45 PM	**TPS Research Session 2: Attacks and Defenses on AI Models** (Room: King's Garden 5) Session Chair: Liyue Fan, UNC-Charlotte (USA)	**CogMI Research Session 2: AI Privacy, Security & Robustness** (Room: King's Garden 2) Session Chair: Reza Zafarani, Syracuse University (USA)	**Invited TPS/CIC/CogMI Session 1:** (Room: King's Garden 3) Session Chair: Wenqi Wei, Fordham University (USA)
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 Light Breakfast (King's Garden 4)		
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 3** (Room: King's Garden 5) **Huan Liu, Arizona States University, USA** **Title: Ceaseless Inquiries - Lesson Learned from Social Media Mining** (Chair: Paolo Boldi, Università degli Studi di Milano, Italy)		
9:45 AM – 10:00 AM	**Coffee Break** (King's Garden 5)		
10:00 AM – 12:00 AM	**TPS Research Session 3: Generative AI, Risks, Attacks, and Defenses** (Room: King's Garden 5) Session Chair: Chidi Agbo, University of Nebraska at Kearney (USA)	**CogMI Research Session 3: AI for Human Wellbeing, Education & Healthcare** (Room: King's Garden 2) Session Chair: Alina Vereshchaka, University at Buffalo (USA)	**Invited TPS/CIC/CogMI Session 2:** (Room: King's Garden 3) Session Chair: Indrajit Ray, Colorado State University (USA)
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's Garden 5) **Dimitrios Gerogakopolous, ARC Industrial Transformation Research Hub for Future Digital Manufacturing, Australia and 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: Wenqi Wei, Fordham University, USA)		
02:00 PM – 3:30 PM	**Panel 2** (Room: King's 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 (Carnegie Mellon University, USA), Amarda Shehu (George Mason University, USA), Jialie (Jerry) Shen (City St George's, University of London, UK) and Huan Liu, (Arizona States University, USA) **Moderator:** *Paolo Boldi, Università degli Studi di Milano, Italy*		
03:30 PM – 03:45 PM	**Coffee Break** (Room: King's Garden 5)		
03:45 PM – 05:45 PM	**TPS Research Session 4: Emerging Frontiers in Security and Trust** (Room: King's Garden 5) Session Chair: Chirag Agrawal, Novelis (USA)	**CogMI Research Session 4: Applied AI, Multimodality & Emerging Paradigms** (Room: King's Garden 2) Session Chair: Paolo Boldi, Università degli Studi di Milano (Italy)	**Invited TPS/CIC/CogMI Session 3:** (Room: King's Garden 3) Session Chair: Danda B. Rawat, Howard University (USA)
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 Light Breakfast (King's Garden 4)			
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, University of Texas at Dallas, USA** **Title: Artificial Intelligence for Transportation Systems Security and Resiliency** **Chair:** Elisa Bertino, Purdue University, USA			
9:45 AM – 10:00 AM	Coffee Break (King's Garden 5)			
10:00 AM – 12:00 AM	**TPS Research/Application Session 5: Privacy and Trust in AI & Collaborative Learning** (Room: King's Garden 5) Session Chair: Imraul Emmaka, University of Arkansas at Little Rock (USA)	**CogMI Research/Application Session 5: Applied AI for Systems, Security & Automation** (Room: King's garden 2) Session Chair: Paolo Boldi, Università degli Studi di Milano (Italy)	**Invited TPS/CIC/CogMI Session 4:** (Room: King's Garden 3) Session Chair: Yanzhao Wu, Florida Intl Univ. (USA)	**Invited TPS/CIC/CogMI Session 5:** (Room: Kings Garden 1) Session Chair: Yanzhao Wu, Florida International University (USA)
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, Google (New York), USA** **Title: Practical Considerations for Differential Privacy and what it means for LLMs** (Chair: Balaji Palanizamy, University of Pittsburgh, USA)			
02:00 PM – 3:30 PM	**Panel 3** (Room: King's garden 5) **Panel Title: IEEE CIC Panel: Device, Data and Collaboration – the Emerging Challenges in Internet of "Intelligent" Things** **Panelists**: *Robert* K. Cunningham (University of Pittsburgh, USA), Indrakshi Ray (University of Colorado, USA), Mahadev Satyanarayanan (Carnegie Mellon University, USA), Bhavani Thuraisingham (University of Texas at Dallas, USA) **Moderator:** *Calton Pu, Georgia Institute of Technology, USA*			
03:30 PM – 03:45 PM	**Coffee Break (**King's Garden 5)			
03:45 PM – 05:45 PM	**TPS Application Session 6: Vulnerability Detection and Security Defense Mechanisms** (Room: King's Garden 5) Session Chair: Imraul Emmaka, University of Kentucky (USA)	**CogMI Application/Research Session 6: Cognitive Intelligence, Quantum & Scientific Applications** (Room: King's garden 2) Session Chair: Naeem Ul Islam, Yuan Ze University (Taiwan)	**CIC Research/Application Session 2: Securing AI, Data, and Systems** (Room: King's Garden 3) Session Chair: Souradip Nath, Arizona State University (USA)	**Tutorial on Data Economics: Incentives, Privacy Tensions, and Fairness Considerations** (Room: Kings Garden 1) Presenter: Juba Ziani, Georgia Tech
05:45 PM –6:00 PM	**Closing remarks** (King's Garden 5)			

IEEE 2025 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's Garden 5

Keynote 1 (Room: King's 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

10:00 am – 12:00 noon
Room: King's Garden 5
Session Chair: Bruhadeshwar Bezawada, Southern Arkansas University (USA)

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's Garden 3
Session Chair: Balaji Palanisamy, University of Pittsburgh, USA

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)

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)

Novel Applications of Blockchain-based Timed Data Release
Jingzhe Wang (University of Pittsburgh) and Balaji Palanisamy (University of Pittsburgh)

CogMI Research Session 1: Reasoning, Agents & Reinforcement Learning

Time: 10:00am – 12noon
Room: King's garden 2
Session Chair: Reza Zafarani, Syracuse University (USA)

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

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

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

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

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

Online Decision Mamba
Trenton Ruf (Portland State University) and Banafsheh Rekabdar (Portland State University)

Lunch Break

12:00 PM – 1:00 PM (Room: King's Garden 4)

Keynote 2 (Room: King's 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: Danda B. Rawat, Howard University, USA

Panel 1 Session (Room: King's Garden 5)

02:00 PM – 03:30 PM
Panel Title: IEEE TPS Panel: Towards building Trustworthy and Responsible Agentic AI
Panelists: Elisa Bertino (Purdue University, USA), Matthew Gaston (Carnegie Mellon University Software Engineering Institute, USA), Heiko Ludwig (IBM Research, USA) and Ling Liu (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's Garden 5
Session Chair: Liyue Fan, UNC-Charlotte (USA)

Robust Physically Realizable Backdoor Attack
Md Jahirul Islam (Kennesaw State 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 TPS/CIC/CogMI Session 1: Federated, Distributed, and Scalable AI Systems

Time: 3:45pm – 5:45pm
Room: King's Garden 3
Session Chair: Wenqi Wei, Fordham University (USA)

FedHFT: Efficient Federated Fine-tuning with Heterogeneous Edge Clients
Fatih Ilhan (Georgia Institute of Technology, USA), Selim Furkan Tekin (Georgia Institute of Technology, USA), Tiansheng Huang (Georgia Institute of Technology, USA), Gaowen Liu (Cisco Research, USA), Ramana Kompella (Cisco Research, USA), Greg Eisenhauer (Georgia Institute of Technology, USA), Yingyan Celine Lin (Georgia Institute of Technology, USA), Calton Pu (Georgia Institute of Technology, USA), Ling Liu (Georgia Institute of Technology, USA)

Agentic LLM-Assisted Edge AI for CPS/IoT Applications
Jinyang Li (University of Illinois Urbana-Champaign, USA), Herman Wu (University of Illinois Urbana-Champaign, USA), Hongjue Zhao (University of Illinois Urbana-Champaign, USA), Tomoyoshi Kimura (University of Illinois Urbana-Champaign, USA), Denizhan Kara (University of Illinois Urbana-Champaign, USA), Tianshi Wang (University of Illinois Urbana-Champaign, USA),

Yizhuo Chen (University of Illinois Urbana-Champaign, USA), Tianchen Wang (University of Illinois Urbana-Champaign, USA), Yigong Hu (University of Illinois Urbana-Champaign, USA), Ashitabh Misra (University of Illinois Urbana-Champaign, USA), Tarek Abdelzaher (University of Illinois Urbana-Champaign, USA)

Rethinking Big Data Scale: Balancing Accuracy, Collaboration, and Storage
Panos K. Chrysanthis (University of Pittsburgh, USA), Constantinos Costa (Rinnoco Ltd, Cyprus)

Toward User Preference Alignment in LLM Recommendation via Explicit Context Feedback
Weizhi Zhang (University of Illinois Chicago, USA; Meta, USA), Wooseong Yang (University of Illinois Chicago, USA), Yuxin Cui (Meta, USA), Zhaohui Guo (Meta, USA), Hins Hu (Meta, USA), Liangwei Yang (University of Illinois Chicago, USA), Henry Peng Zou (University of Illinois Chicago, USA), Qifei Wang (Meta, USA), Hanqing Zeng (Meta, USA), Jiayi Liu (Meta, USA), Yinglong Xia (Meta, USA), Philip S. Yu (University of Illinois Chicago, USA)

Augmenting Question Answering with a Hybrid RAG Approach
Tianyi Yang (Fordham University, USA), Nashrah Haque (Fordham University, USA), Vaishnave Jonnalagadda (Fordham University, USA), Yuya Jeremy Ong (Plastic Lab, USA), Zhehui Chen (Google, USA), Yanzhao Wu (Florida International University, USA), Lei Yu (Rensselaer Polytechnic Institute, USA), Divyesh Jadav (Independent Consultant), Wenqi Wei (Fordham University, USA)

CogMI Research Session 2: AI Privacy, Security & Robustness

Time: 3:45pm – 5:45pm
Room: King's garden 2
Session Chair: Reza Zafarani, Syracuse University (USA)

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

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

Edge-Optimized Privacy: Synthetic Data Generation Using Hybrid SMOTE & Autoencoder
Kiana Katouzian (North Carolina A&T State University) and Ahmad Patooghy (North Carolina A&T State University)

RL-MoE: An Image-Based Privacy Preserving Approach In Intelligent Transportation System
Abdolazim Rezaei (Texas A&M University Corpus Christi), Mehdi Sookhak (Texas A&M University Corpus Christi) and Mahboobeh Haghparast (Texas A&M University Corpus Christi)

Deep Metric Stylometry: Learning Author Signatures from Style and Semantics
Mostafa Rahgouy (Department of Computer Science and Software Engineering, Auburn University), Mehnaz Tabassum (Office of Information Technology, Auburn University), Amit Das (University of North Alabama), Dongji Feng (Department of Mathematics, Computer Science, and Statistics,

Gustavus Adolphus College), Gerry Dozier (Department of Computer Science and Software Engineering, Auburn University) and Cheryl D. Seals (Department of Computer Science and Software Engineering, Auburn University)

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

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

Networking/Reception (provided by the conference**)**
Room: King's Garden Foyer
06:00 PM – 09:00 PM

IEEE 2025 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's Garden 5

Keynote 3 (Room: King's 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: Paolo Boldi, Università degli Studi di Milano, taly

Coffee Break (15 min)

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

Time: 10:00am – 12noon
Room: King's Garden 5
Session Chair: Chidi Agbo, University of Nebraska at Kearney (USA)

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: Alina Vereshchaka, University at Buffalo (USA)

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

Dynamic Stress Detection: A Study of Temporal Progression Modelling of Stress in Speech
Vishakha Lall (Centre of Excellence in Maritime Safety, Singapore Polytechnic) and Yisi Liu (Centre of Excellence in Maritime Safety, Singapore Polytechnic)

Uncertainty-Aware Temporal Modeling for Student Dropout Prediction in Online Learning Environments
Ikram Gagaoua (RiseUp, Université de Lorraine, CNRS, LORIA)

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

ELM: Leveraging Large Language Models for Reliable Emotion Recognition
Richard Feng (St. Margaret's Episcopal School)

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

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

Invited TPS/CIC/CogMI Session 2: Security, Privacy, and Trust in AI Systems

Time: 10:00am – 12noon
Room: King's Garden 3
Session Chair: Indrajit Ray, Colorado State University (USA)

Security of Operations on Random Numbers
Tejas Sharma (IIT Bombay, India), Ashish Kundu (Cisco Research, USA)

Experiences Building Enterprise-Level Privacy-Preserving Federated Learning to Power AI for Science
Zilinghan Li (Argonne National Laboratory, USA; University of Illinois Urbana-Champaign, USA), Aditya Sinha (Argonne National Laboratory, USA; National Center for Supercomputing Applications (NCSA), USA; University of Illinois Urbana-Champaign, USA), Yijiang Li (Argonne National Laboratory, USA), Kyle Chard (Argonne National Laboratory, USA; University of Chicago, USA), Kibaek Kim (Argonne National Laboratory, USA; University of Chicago, USA), Ravi Madduri (Argonne National Laboratory, USA; University of Chicago, USA)

GBP-Audit: AI Bias Intervention with Built-In Safety-First Guardrails
Ronald Doku (Haske Labs, USA; Howard University, USA), Nana Yaw A. Osafo (Howard University, USA), Danda B. Rawat (Howard University, USA)

Detection of Blacktopped Counterfeit ICs Using Surface Texture Analysis
John M. Klamut (University of Pittsburgh, USA), Mai Abdelhakim (University of Pittsburgh, USA), Samuel J. Dickerson (University of Pittsburgh, USA), Ashish Avachat (University of Pittsburgh, USA), Heng Ban (University of Pittsburgh, USA), Philip Santillo (University of Pittsburgh, USA)

Can We Align LLMs We Don't Understand? A Call for User-Centric Interpretability
Zhen Tan (Arizona State University, USA), Huan Liu (Arizona State University, USA)

Lunch Break

12:00 PM – 1:00 PM (Room: King's Garden 4**)**

Keynote 4 (Room: King's 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: Wenqi Wei, Fordham University, USA

Panel 2 Session (Room: King's 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 (Carnegie Mellon University, USA), Amarda Shehu (George Mason University, USA), Jialie (Jerry) Shen (City St George's, University of London, UK) and Huan Liu, (Arizona States University, USA)
Moderator: Paolo Boldi, Università degli Studi di Milano, Italy

Coffee Break (15 min)

TPS Research Session 4: Emerging Frontiers in Security and Trust

Time: 3:45pm – 5:45pm
Room: King's Garden 5
Session Chair: Chirag Agrawal, Novelis (USA)

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 Face 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: Paolo Boldi, Università degli Studi di Milano (Italy)

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

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

Cross-Country Analysis of Discourse on Misinformation in the Digital Platform Using Topic Modeling
Minh Nguyen (Florida Atlantic University), Kuheli Sai (University of Pittsburgh), Deepti Gupta (Texas A&M University, Central Texas) and Quang-Thinh Bui (Tien Giang University)

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

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

Explaining at the Speed of Sight: Attention-Aware XAI for OODA-Inspired AI Design
Dylan Wright (University of Alabama in Huntsville (Graduate Student)) and Vineetha Menon (University of Alabama in Huntsville)

ConvFormer: A Strong Convolutional Baseline for Multi-Agent Trajectory Prediction
Yury Davydov (National Taipei University of Technology), Wen-Hui Chen (National Taipei University of Technology) and Yu-Chen Lin (Department of Automatic Control Engineering, Feng Chia University)

Invited TPS/CIC/CogMI Session 3: Secure Collaborative Data Intelligence

Time: 3:45pm – 5:45pm
Room: King's Garden 3
Session Chair: Danda B. Rawat, Howard University (USA)

Revisiting the Inference Problem in Database Security in the Era of Artificial Intelligence
Bhavani Thuraisingham (The University of Texas at Dallas, USA)

Collaborative Research on Nonprofits: Broadening Knowledge with New Data Management
Calton Pu (Georgia Institute of Technology, USA), Lewis Faulk (American University, USA)

Multi-modal, federated AI for cancer prognosis and treatment optimization
Chalapathy Neti (Yorktown Heights, USA)

Banquet Dinner (provided by the conference)

Room: King's Garden 4
06:00 PM – 09:00 PM

IEEE 2025 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's Garden 5

Keynote 5 (Room: King's 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: Elisa Bertino, Purdue University, USA

Coffee Break (15 min)

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

Time: 10:00am – 12noon
Room: King's Garden 5
Session Chair: Imraul Emmaka, University of Arkansas at Little Rock (USA)

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: Paolo Boldi, Università degli Studi di Milano (Italy)

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

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

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

Human-in-the-Loop Runbook Improvement with Agentic Support Automation
Rocker D'Antonio (Mississippi State University) and Harry Xie (Amazon Web Services)

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

Dynamic Reward Scaling for Multivariate Time Series Anomaly Detection: A VAE-Enhanced Reinforcement Learning Approach (Application-Track)
Bahareh Golchin (Department of Computer Science, Portland State University) and Banafsheh Rekabdar (Department of Computer Science, Portland State University)

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

Invited TPS/CIC/CogMI Session 4: Trustworthy and Sustainable AI

Time: 10:00am – 12noon
Room: King's Garden 3
Session Chair: Yanzhao Wu, Florida Intl Univ. (USA)

The Impact of Generative AI in Renewable Energy Applications
Jialie Shen (City St George's, University of London, UK), Haiyan Miao (University of Huddersfield, UK), Fengshou Gu (University of Huddersfield, UK))

Upgrade or Switch: Do We Need a Next-Gen Trusted Architecture for the Internet of AI Agents?
Ramesh Raskar (MIT, USA), Pradyumna Chari (MIT, USA), Mahesh Lambe (Independent Researcher, USA), Robert Lincourt (Dell Technologies, USA), Raghu Bala (Synergetics AI, USA), Aditi Joshi (Independent Researcher, USA), Jared James Grogan (Independent Researcher, USA), Abhishek Singh (MIT, USA), Ayush Chopra (MIT, USA), Rajesh Ranjan (Independent Researcher, USA), Shailja Gupta (Independent Researcher, USA), Dimitris Stripelis (Flower AI, UK), Maria Gorskikh (Independent Researcher), Sichao Wang (Cisco Systems, USA)

Towards Mobile AI That Is Accurate and Fast
Mahadev Satyanarayanan (Carnegie Mellon University, USA), Qifei Dong (Carnegie Mellon University, USA), Jingao Xu (Carnegie Mellon University, USA), Padmanabhan Pillai (Carnegie Mellon University, USA)

Toward Carbon-Neutral Human AI: Rethinking Data, Computation, and Learning Paradigms for Sustainable Intelligence
KC Santosh (University of South Dakota, USA), Rodrigue Rizk (University of South Dakota, USA), Longwei Wang (University of South Dakota, USA)

Invited TPS/CIC/CogMI Session 5: Applied AI, Analytics, and Reasoning

Time: 10:00am – 12noon
Room: Kings Garden 1
Session Chair: Yanzhao Wu, Florida International University (USA)

A Comparison of Rank-Ordering and Classification for Occupational Injury Absence Duratio
Chelsea M. Zuvieta (Florida Atlantic University, USA), Gonzalo A. Vivian (Florida Atlantic University, USA), Taghi M. Khoshgoftaar (Florida Atlantic University, USA)

Challenges in Identifying Illicit Actors in Financial Networks
Amro A. Aljundi (University of Virginia, USA), Abhijin Adiga (University of Virginia, USA), Philip B. K. Potter (University of Virginia, USA), Samarth Swarup (University of Virginia, USA), Anil Vullikanti (University of Virginia, USA), Madhav V. Marathe (University of Virginia, USA)

Unlocking Machine Learning Insights into a Novel Auto Repossession Dataset
Andy Sinclair (Florida Atlantic University, USA), Preston Billion-Polak (Florida Atlantic University, USA), Taghi M. Khoshgoftaar (Florida Atlantic University, USA)

Enhancing the Robustness of AI-Generated Voice Detectors Against Data Poisoning Attacks
Ian Miller (Vanderbilt University, USA), Ke Li (Vanderbilt University, USA), Dan Lin (Vanderbilt University, USA)

Research on Causal Casualty Outcomes and Vulnerabilities using Reasoning (REC2OVR)
Adrienne Raglin (ARL), Brian Vincent (ARL)

Lunch Break

12:00 PM – 1:00 PM (Room: King's Garden 4)

Keynote 6 (Room: King's 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: Balaji Palanisamy, University of Pittsburgh, USA)

Panel 3 Session (Room: King's Garden 5)

02:00 PM – 03:30 PM
Panel Title: IEEE CIC Panel: Device, Data and Collaboration – the Emerging Challenges in Internet of "Intelligent" Things
Panelists: Robert K. Cunningham (University of Pittsburgh, USA), Indrakshi Ray (University of Colorado, USA), Mahadev Satyanarayanan (Carnegie Mellon University, USA), Bhavani Thuraisingham (University of Texas at Dallas, USA)
Moderator: Calton Pu, Georgia Institute of Technology, USA

Coffee Break (15 min)

TPS Application Session 6: Vulnerability Detection and Security Defense Mechanisms

Time: 3:45pm – 5:45pm
Room: King's Garden 5
Session Chair: Imraul Emmaka, University of Kentucky (USA)

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 (École de l'air et de l'espace), Kayla D. Taylor (Embry-Riddle Aeronautical University), Laxima Niure Kandel (Embry-Riddle Aeronautical University), Deepti Gupta (Texas A&M University–Central Texas)

VulnDetective: Using LLM Agents to Analyze Common Weaknesses and Identify Smart Contract Vulnerabilities
Thanmai Mandala (University of Texas at Dallas), Cora Zeger (University of Denver), Tessa Andersen (Brigham Young University), Gaby G. Dagher (Boise State University), Jun Zhuang (Boise State University)

XAST: Explainable AST-Transformer for Smart Contract Vulnerability Detection
Harshith Sai Veeraiah (California State University, Sacramento), Syed Badruddoja (California State University, Sacramento), 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's Garden 3
Session Chair: Souradip Nath, Arizona State University (USA)

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: Naeem Ul Islam, Yuan Ze University (Taiwan)

MORAL: A Multimodal Reinforcement Learning Framework for Cognitive Intelligence in Autonomous Laboratories

Natalie Tirabassi (Cleveland State University), Sathish Kumar (Cleveland State University), Sumit Jha (Florida International University) and Arvind Ramanathan (Argonne National Laboratory)

The Imitation Fallacy: Why Behavioral Equivalence Cannot Verify Artificial Consciousness
Aayush Gauba (Southern Illinois University Edwardsville)

Quantum Regression for Cognitive Intelligence in Complex Environments
Ahmad Alomari (Cleveland State University) and Sathish Kumar (Cleveland State University).

Robust and Efficient Traffic Monitoring System Under Adverse Weather
Ramy Othman (Montclair State University), Anisha Mulinti (Montville Township High School), William O'Donnell (Montclair State University), Weitian Wang (Montclair State University) and Michelle Zhu (Montclair State University)

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

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

Tutorial on Data Economics: Incentives, Privacy Tensions, and Fairness Considerations

Time: 3:45pm – 5:45pm
Room: Kings Garden 1
Presenter: Juba Ziani, Gergoa Tech, USA

Closing Remarks

5:45pm – 6:00pm
Room: **King's Garden 5**