# IEEE 2024 CIC/COGMI/TPS JOINT CONFERENCES

# CONFERENCE PROGRAM

The Darcy Hotel, Washington D.C., USA
October 28 - 30, 2024

VERSION
Sept 14

## Useful Resources

**Conference Website**

- CIC: http://www.sis.pitt.edu/lersais/conference/cic/2024/
- TPS: http://www.sis.pitt.edu/lersais/conference/tps/2024/
- CogMI: http://www.sis.pitt.edu/lersais/conference/cogmi/2024/

# Overview Day 1: Monday, Oct 28, 2024

| | | | | | |
|---|---|---|---|---|---|
| 7:15 AM - 8:30 AM | | Registration & Continental Breakfast (provided by conference) | | | |
| 8:30 AM - 8:45 AM | | **Welcome and Opening Remarks**<br>(Steering Committee Chair and Organizing Committee Chairs)<br>(Room: Logan Ballroom) | | | |
| 08:45 AM – 9:45 AM | **Workshop**<br>**(LLM CyberSec)**<br>(Room: Deacon)<br>**Chair**: Kristen Moore (CSIRO) | **Keynote 1** (Room: Logan Ballroom)<br>**Jeannette M. Wing**, *Executive Vice President for Research & Professor of Computer Science, Columbia University*<br>**Title: Trustworthy AI**<br>(Chair: James Joshi, University of Pittsburgh, USA) | | | |
| 09:45 AM – 10:45 AM | | **Keynote 2** (Room: Logan Ballroom)<br>**Deirdre K. Mulligan**, *Director of the Berkeley Center for Law and Technology & Professor, School of Information, UC Berkeley*<br>**Title: New Directions in Tech Governance**<br>(Chair: James Joshi, University of Pittsburgh, USA) | | | |
| 10:45 AM – 11:00 AM | | Break | | | |
| 11:00 AM – 12:20 AM | | **TPS Invited Research/Vision Session 1: Malware Detection, Forensics, and Deep Learning**<br>(Room: Logan Ballroom)<br>Session Chair: Amir Masoumzadeh (SUNY-Albany, US) | **CogMI Invited Research/Vision Session 1: Causal Inference, AI, and Logical Reasoning**<br>(Room: Gaston)<br>Session Chair: Julian Jarrett (Lutron Electronics, US) | **CIC Invited Research/Vision Session 1: AI for Autonomous Systems, Security, and Monitoring**<br>(Room: Bader)<br>Session Chair: Mei-Ling Shyu (UMKC, US) | **Workshop**<br>**(Inclusive AI)**<br>(Room: Whitman)<br>**Chairs** Hemant Purohit (GMU), Jin-Hee Cho (Virginia Tech), Yoosun Chung (GMU) |
| 12:20 PM – 01:30 PM | 12:20 PM – 1:30 PM | **Lunch Break** (provided by conference) | | | |
| 01:30 PM – 02:30 PM | **Workshop**<br>**(LLM CyberSec)**<br>(Room: Deacon)<br>**Chair**: Kristen Moore (CSIRO) | **Keynote 3** (Room: Logan Ballroom)<br>**Ed H. Chi**, *Distinguished Scientist & Research Lead (LLM/LaMDA), Google DeepMind*<br>**Title: The Future of Discovery Assistance**<br>(Chair: Huan Liu, Arizona State University, USA) | | | |
| 02:30 PM – 04:30 PM | | **Panel 1** (Room: Logan Ballroom)<br>**Panel Title: How Will Artificial Intelligence Reshape Scientific Research?**<br>**Panelists**: *Li Yang (National Science Foundation, US), Hemant Purohit (George Mason Univ, US), Ling Liu (Georgia Tech, US), Huan Liu (ASU, US), Ed Chi (Google, US)*<br>**Moderator:** *Paolo Boldi, University of Milan, Italy* | | | |
| 04:30 PM – 04:45 PM | | **Coffee Break** | | | |
| 04:45 PM – 06:25 PM | | **TPS Session 1: Privacy Enhancing Technologies and Cybersecurity Threats**<br>(Room: Logan Ballroom)<br>Session Chair: Lavanya Elluri (TAMU-Central Texas, US) | **CogMI Session 1: AI-enhanced security, and automated monitoring**<br>(Room: Gaston)<br>Session Chair: Julian Jarrett (Lutron Electronics, US) | **CIC Session 1: AI-powered Systems and Applications**<br>(Room: Bader)<br>Session Chair: Latifur Khan (UT Dallas, USA) | **Workshop**<br>**(Inclusive AI)**<br>(Room: Whitman) |
| 06:30 PM – 08/09:00 PM | | **Networking/Reception** (provided by conference) | | | |

# Overview Day 2: Tuesday, Oct 29, 2024

| | | | | | |
|---|---|---|---|---|---|
| 7:15 AM - 8:30 AM | | Registration & Continental Breakfast | | | |
| 8:30 AM - 8:45 AM | | **Remarks and Conference Logistics**<br>(Room: Logan Ballroom) | | | |
| 8:45 AM – 9:45 AM | **Workshop (QUILLS)**<br>(Room: Deacon)<br>**Chairs:** Kaushik P. Seshadreesan (University of Pittsburgh) | **Keynote 4** (Room: Logan Ballroom)<br>**Michael L. Littman**, NSF IIS Division Director & University Professor of Computer Science, Brown University<br>Title**: The National Science Foundation's Role in the Future of AI**<br>(Chair: *Jaideep Vaidya, Rutgers University, USA*) | | | |
| 9:45 AM – 10:00 AM | | Break | | | |
| 10:00 AM – 12:00 PM | | **TPS Session 2: Large Language Models for Privacy and Security**<br>(Room: Logan Ballroom)<br>Session Chair: Indrajit Ray (CSU, USA) | **CogMI Invited Research/Vision Session 2: Systems, Applications, and AI Performance**<br>(Room: Gaston)<br>Session Chair: Keke Chen (UMBC, USA) | **CIC Session 2: AI-driven Systems, Security and Computing**<br>(Room: Badar)<br>Session Chair: Barbara Carminati (University of Insubria, Italy) | **TPS Invited Research/Vision Session 2: AI, Quantum Computing, and Cybersecurity**<br>(Room: Whitman)<br>Session Chair: Amir Masoumzadeh (SUNY-Albany, US) |
| 12:00 PM – 02:00 PM | | Lunch Break (provided by conference) and<br>**Panel Session** (Room: Logan Ballroom)<br>**Student Mentoring Panel**<br>**Tiny Keynote: Jaideep Vaidya (Rutgers University, USA)**<br>**Panelists:** Jaideep Vaidya (Rutgers University, USA), Huan Liu (Arizona State University, USA), Indrakshi Ray (Colorado State University, USA), Stacey Truex (Denison University, USA), Peter Kairouz (Google, USA), Ambareen Siraj (SFS/SaTC Program, NSF, USA*)*<br>**Moderator:** *Wenqi Wei*, Fordham University, USA | | | |
| 02:00 PM – 03:00 PM | **Workshop (QUILLS)**<br>(Room: Deacon)<br>**Chairs:** Kaushik P. Seshadreesan (University of Pittsburgh) | **Keynote 5** (Room: Logan Ballroom)<br>**Roshan Thapliya**, Corporate Officer, Chief Digital Transformation Officer and General Manager, TDK Corporation, Tokyo, Japan<br>Title: **Transforming Society: TDK's Vision Accelerated by Digital Transformation**<br>(Chair: James Joshi, University of Pittsburgh, USA) | | | |
| 03:00 PM – 03:15 PM | | Break | | | |
| 03:15 PM – 05:15 PM | | **TPS Session 3: Privacy and Security in AI/ML**<br>(Room: Logan Ballroom)<br>Session Chair: Dipankar Dasgupta (University of Memphis, US) | **CogMI Session 2: AI-driven decision-making and human-centered systems**<br>(Room: Gaston)<br>Session Chair: Keke Chen (UMBC, US) | **CogMI Session 3: AI and Language Models for human-centered systems**<br>(Room: Badar)<br>Session Chair: Kim Hemmings-Jarrett (PSU, US) | **TPS Invited Research/Vision Session 3: AI Security, Privacy, and Healthcare**<br>(Room: Whitman)<br>Session Chair: Indrakshi Ray (CSU, US) |
| 06:00 PM – 09:00 PM | | **Banquet Dinner** (provided by conference) | | | |

# Overview Day 3: Wednesday, Oct 30, 2024

| | | | | | |
|---|---|---|---|---|---|
| 07:15 AM - 08:00 AM | Registration & Continental Breakfast (provided by conference) | | | | |
| 08:00 AM – 10:00 AM | **Workshop (WAAM)**<br>(Room: Deacon)<br>**Chairs:** Phil LaPlante (NIST) and Rick Kuhn (NIST) | **Workshop (SR-CIST)**<br>(Room: Gaston)<br>**Chairs:** Mai Abdelhakim (University of Pittsburgh), Mohan Baruwal Chhetri (CSIRO), Peilin He (University of Pittsburgh) | **TPS Session 4: Malware and Threat Detection**<br>(Room: Logan Ballroom)<br>Session Chair: Pooria Madani (OntarioTechU, Canada) | **CogMI Session 4: AI-driven modeling and analysis for behavioral and network systems**<br>(Room: Badar)<br>Session Chair: Yanzhao Wu (FIU, USA) | **Workshop (EIC)**<br>(Room: Whitman)<br>**Chairs:** Julian Jarrett (Lutron Electronics, US) |
| 10:00 AM – 10:15 AM | | | Break | | |
| 10:15 AM – 12:15 PM | | | **Panel 2** (Room: Logan Ballroom)<br>Panel Title: Driving Innovations in Emerging Technologies: R&D Priorities and Funding Landscape<br>**Panelists**: Jennifer Roberts (Director, Resilient Systems, ARPA-H, USA), Heidi Sofia (Deputy Director, NCBI-NIH, USA), Elham Tabassi (Associate Director of Emerging Technology, NIST, USA), Cliff Wang, (Program Director, SaTC Program, *NSF, USA), Dr. Craig Schlenoff (Director, NITRD + AD of Networking and IT at White House OSTP)*<br>**Moderator:** James Joshi, University of Pittsburgh, USA and Huan Liu, Arizona State University, USA | | |
| 12:15 PM – 01:15 PM | Lunch Break (provided by conference) | | | | |
| 01:15 PM – 03:00 PM | **Workshop (WAAM)**<br>(Room: Deacon)<br>**Chairs:** Phil LaPlante (NIST) and Rick Kuhn (NIST) | **Workshop (SR-CIST)**<br>(Room: Gaston) | **TPS Session 5: Access Control and Security Models**<br>(Room: Logan Ballroom)<br>Session Chair: Wenqi Wei (Fordham University, USA) | | **Tutorial: Tutorial: Computational Scientific Discovery in Cognitive Science**<br>(Room: Whitman)<br>Session Chair: Fernand Gobet |
| 3:00 pm -5:00 pm | | | **Panel 3** (Room: Logan Ballroom)<br>Panel Title: AI vs AI: The Inevitable Next Cyber Frontier<br>**Panelists**: Karl Aberer, (EPFL, Switzerland), Elena Ferrari (University of Insubria, Italy), Anupam Joshi (UMBC, USA), Calton Pu (Georgia Tech, USA), Peter Kairouz (Google, USA)<br>**Moderator:** *James Joshi, University of Pittsburgh, USA* | | |
| 05:00 PM – 05:15 PM | **Closing Remarks**<br>(Room: Logan Ballroom) | | | | |

# IEEE 2024 CIC/CogMI/TPS Joint Conferences
# Day 1: Monday, October 28, 2024

## 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 - Logan Ballroom

## Keynote 1 (Room: Logan Ballroom)

08:45 AM – 9:45 AM
**Jeannette M. Wing,** Executive Vice President for Research & Professor of Computer Science, Columbia University
Title: Trustworthy AI
Session Chair: James Joshi (University of Pittsburgh, USA)

## Keynote 2 (Room: Logan Ballroom)

09:45 AM – 10:45 AM
**Deirdre K. Mulligan**, Director of the Berkeley Center for Law and Technology & Professor, School of Information, UC Berkeley
Title: New Directions in Tech Governance
Session Chair: James Joshi (University of Pittsburgh, USA)

### Coffee Break (15 min)

## TPS Invited Research/Vision Session 1: Malware Detection, Forensics, and Deep Learning

11:00 am – 12:20 pm
Room: Logan Ballroom
Session Chair: Amir Masoumzadeh (SUNY-Albany, US)

**Large Language Models to Enhance Malware Detection in Edge Computing**
Christian Rondanini (University of Insubria), Barbara Carminati (University of Insubria), Elena Ferrari (University of Insubria), Ashish Kundu (Cisco Research) and Akshay Jajoo (Cisco Research)

**Digital Evidence Chain of Custody: Navigating New Realities of Digital Forensics**
Souradip Nath (Arizona State University), Keb Summers (Arizona State University), Jaejong Baek (Arizona State University) and Gail-Joon Ahn (Arizona State University)

**Boosting Imperceptibility of Stable Diffusion-based Adversarial Examples Generation with Momentum**
Nashrah Haque (Fordham University), Xiang Li (Fordham University), Zhehui Chen (Google), Yanzhao Wu (Florida International University), Lei Yu (RPI), Arun Iyengar (Cisco Research) and Wenqi Wei (Fordham University)

**Effective Diversity Optimizations for High Accuracy Deep Ensembles**
Hongpeng Jin (Florida International University), Maryam Akhavan Aghdam (Florida International University), Sai Nath Chowdary Medikonduru (Florida International University), Wenqi Wei (Fordham University), Xuyu Wang (Florida International University), Wenbin Zhang (Florida International

University), Yanzhao Wu (Florida International University)

## CogMI Invited Research/Vision Session 1: Causal Inference, AI, and Logical Reasoning

11:00 am – 12:20 pm

Room: Gaston

Session Chair: Julian Jarrett (Lutron Electronics, US)

**State-Of-The-Art and Challenges in Causal Inference on Graphs: Confounders and Interferences**
Jingyuan Chou (University of Virginia), Jiangzhuo Chen (University of Virginia) and Madhav Marathe (University of Virginia)

**Causal Inductive Biases for Cognitive Machine Learning**
Saketh Vishnubhatla (Arizona State University), Adrienne Raglin (DEVCOM Army Research Laboratory), Raha Moraffah (Worcester Polytechnic Institute) and Huan Liu (Arizona State University)

**Causal Intervention and Semantic Knowledge for Object Relationships**
Ayron Fears (Howard University), Adrienne Raglin (DEVCOM Army Research Laboratory) and Adrienne Raglin (DEVCOM Army Research Laboratory)

**The Case for Micro Foundation Models to Support Robust Edge Intelligence**
Tomoyoshi Kimura (University of Illinois at Urbana-Champaign), Yizhuo Chen (University of Illinois at Urbana-Champaign), Denizhan Kara (University of Illinois at Urbana-Champaign), Jinyang Li (University of Illinois at Urbana-Champaign), Tianshi Wang (University of Illinois at Urbana-Champaign), Ruijie Wang (University of Illinois at Urbana-Champaign), Joydeep Bhattacharyya (DEVCOM Army Research Laboratory), Jae Kim (The Boeing Company), Shengzhong Liu (Shanghai Jiao Tong University ), Prashant Shenoy (University of Massachusetts Amherst), Mani Srivastava (University of California, Los Angeles), Maggie Wigness (DEVCOM Army Research Laboratory) and Tarek Abdelzaher (University of Illinois at Urbana-Champaign)

## CIC Invited Research/Vision Session 1: AI for Autonomous Systems, Security, and Monitoring

11:00 am – 12:20 pm

Room: Ellington

Session Chair: Mei-Ling Shyu (UMKC, USA)

**Autonomous Shuttle Operation for Vulnerable Populations: Lessons and Experiences**
Ren Zhong (Wayne State University), Zhaofeng Tian (University of Delaware), Jinghui Liao (Southern University of Science and Technology) and Weisong Shi (University of Delaware)

**Graphene: Towards Data-driven Holistic Security Posture Analysis using AI-generated Attack Graphs**
Xin Jin (The Ohio State University), Charalampos Katsis (Purdue University), Fan Sang (Georgia Institute of Technology), Jiahao Sun (Georgia Institute of Technology), Elisa Bertino (Purdue University), Ramana Rao Kompella (Cisco Research) and Ashish Kundu (Cisco Research)

**Towards Contactless Human Concentration Monitoring Using mmWave Signals**
Yuan Ge (George Mason University), Yi Wei (George Mason University), Xiaonan Guo (George Mason University), Yucheng Xie (Yeshiva University), Yan Wang (Temple University), Jerry Cheng (New York Institute of Technology) and Yingying Chen (Rutgers University)

**Realizing IoT Sensor Discovery, Payment, and Utilization via an Open Source Sensor Sharing**

**Marketplace**
Dimitrios Georgakopoulos (Swinsburne University of Technology) and Anas Dawod Alrefaee (Swinsburne University of Technology)

## Lunch Break and Panel Session

12:20 PM – 1:30 PM

## Keynote 3 (Room: Logan Ballroom)

01:30 PM – 02:30 PM
**Ed H. Chi,** Distinguished Scientist & Research Lead (LLM/LaMDA), Google DeepMind
Title: **The Future of Discovery Assistance**
Chair: Huan Liu (Arizona State University, USA)

## Panel Session (Room: Logan Ballroom)

02:30 PM – 04:30 PM
Penal Title: **How Will Artificial Intelligence Reshape Scientific Research?**
**Panelists**: Jonathan Gryak (CUNY, US), Hemant Purohit (George Mason Univ, US), Ling Liu (Georgia Tech, US), Huan Liu (ASU, US), Li Yang-TBD (NSF, US)
**Moderator**: Paolo Boldi, University of Milan, Italy

## Coffee Break (15 min)

## TPS Session 1: Privacy Enhancing Technologies and Cybersecurity Threats

04:45 PM – 06:25 PM
Room: Logan Ballroom
Session Chair: Lavanya Elluri (TAMU-Central Texas, US)

**Distributed, Privacy-Aware Location Data Aggregation**
Maja Schneider (ScaDS.AI Dresden/Leipzig), Erik Buchmann (ScaDS.AI Dresden/Leipzig) and Erhard Rahm (ScaDS.AI Dresden/Leipzig)

**Utility-Privacy Aware Mobile Diminished Reality Framework for 3D Visual Privacy**
Salam Tabet (American University of Beirut), Ayman Kayssi (American University of Beirut) and Imad H. Elhajj (American University of Beirut)

**A Privacy-Preserving Cyber Threat Intelligence Sharing System**
Philip Huff (University of Arkansas at Little Rock), Sri Nikhil Gupta Gourisetti (University of Arkansas at Little Rock), Spencer Massengale (University of Arkansas at Little Rock) and Tran Viet Xuan Phuong (University of Arkansas at Little Rock)

**Improved Ethereum Fraud Detection Mechanism with Explainable Tabular Transformer Model**
Ruth Olusegun (Bowie State University) and Bo Yang (Bowie State University)

**Unsupervised Approach for Electricity Theft Detection Combining Recurrent Neural Networks and Rule-Based Policy**
Ashley Ajuz (University of Pittsburgh) and Mai Abdelhakim (University of Pittsburgh)

## CogMI Session 1: AI-enhanced security, and automated monitoring

04:45 PM – 06:25 PM
Room: Gaston
Session Chair: Julian Jarrett (Lutron Electronics, US)

**Enhancing Federated Learning Security: Combating Clients' Data Poisoning with Classifier Ensembles**
Arunava Roy (The University of Memphis) and Dipankar Dasgupta (The University of Memphis).

**Optimized Machine Learning Based Multimodal UAV Detection Using Ensemble Stacking**
James McCoy (Howard University) and Danda Rawat (Howard University).

**Using Automated Core and Spurious Features Detection in Scene Recognition to Explain Computer Vision Model**
Anjon Basak (Stormfish Scientific Corporation) and Adrienne Raglin (DEVCOM Army Research Lab)

**Towards Effective Authorship Attribution: Integrating Class-Incremental Learning**
Mostafa Rahgouy (Department of Computer Science and Software Engineering, Auburn University), Hamed Babaei Giglou (TIB Leibniz Information Centre for Science and Technology), Mehnaz Tabassum (Office of Information Technology, Auburn University), Dongji Feng (Department of Mathematics, Computer Science, and Statistics, Gustavus Adolphus College), Amit Das (Department of Computer Science and Software Engineering, Auburn University), Taher Rahgooy (Menlo Park, CA, USA), Gerry Dozier (Department of Computer Science and Software Engineering, Auburn University) and Cheryl D. Seals (Department of Computer Science and Software Engineering, Auburn University)

**Automated Framework for Groundwater Monitoring Using DWT with LSTM and Transformers**
Mrunmayee Dhapre (San Jose State University), Jehanzeb Khan (San Jose State University), Youngsoo Kim (University of Minnesota Duluth), Thomas Danielson (Savannah River National Laboratory) and Shrikant Jadhav (San Jose State University)

## CIC Session 1: AI-powered Systems and Applications

04:45 PM – 06:25 PM
Room: Ellington
Session Chair: Latifur Khan (UT Dallas, USA)

**Sinema: Semantics-driven Intelligent Network Management using AI assistance**
Thanveer Sulthana (School of Science and Engineering-University of Missouri-Kansas City), Ava Sharif Jourabchi (School of Science and Engineering-University of Missouri-Kansas City), Sejun Song (School of Science and Engineering-University of Missouri-Kansas City) and Baek-Young Choi (School of Science and Engineering-University of Missouri-Kansas City).

**InsightPulse: An IoT-based System for User Experience Interview Analysis**
Dian Lyu (Global Innovation Exchange, University of Washington), Yuetong Lu (Global Innovation Exchange, University of Washington), Jassie He (Global Innovation Exchange, University of Washington), Murad Mehrab Abrar (Department of Mechanical Engineering, University of Washington), Ruijun Xie (Department of Electrical Engineering, George Washington University) and John Raiti (Global Innovation Exchange, University of Washington).

**FGA-IDS: A Federated Learning and GAN-Augmented Intrusion Detection System for UAV Networks**
Qingli Zeng (University of Missouri Kansas City), Semire Olatunde-Salawu (University of Missouri Kansas City) and Farid Nait-Abdesselam (University of Missouri Kansas City).
**A Survey of Transformer Enabled Time Series Synthesis**
Alexander Sommers (Mississippi State University), Logan Cummins (Mississippi State University) and Sudip Mittal (Mississippi State university).

**A Deep Learning Approach to Detect Complete Safety Equipment For Construction Workers Based On YOLOv7**
Md. Shariful Islam (Daffodil International University), Sm Shaqib (Daffodil International University), Shahriar Sultan Ramit (Daffodil International University), Shahrun Akter Khushbu (Daffodil International University), Mr. Abdus Sattar (Daffodil International University) and Dr. Sheak Rashed Haider Noori (Daffodil International University).

## **Networking/Reception (**provided by the conference**)**

06:30 PM – 09:00 PM

# IEEE 2024 CIC/CogMI/TPS Joint Conferences
# Day 2: Tuesday, October 29, 2024

## Registration & Continental Breakfast (provided by the conference)

7:15 AM - 8:30 AM

## Welcome and Opening Remarks

8:30 am – 8:45 am
All Participants and Chairs
Room - Logan Ballroom

## Keynote 4 (Room: Logan Ballroom)

8:45 am – 9:45 am
**Michael L. Littman,** NSF IIS Division Director & University Professor of Computer Science, Brown University
Title: The National Science Foundation's Role in the Future of AI
Chair: Paolo Boldi, (University of Milan, Italy)

## Coffee Break (15 min)

## TPS Session 2: Large Language Models for Privacy and Security

10:00 AM – 12:00 PM
Room: Logan Ballroom
Session Chair: Indrajit Ray (CSU, US)

**Bias Detection and Mitigation in Zero-Shot Spam Classification using LLMs**
Hossein Salemi (George Mason University), Anuridhi Gupta (George Mason University) and Hemant Purohit (George Mason University)

**Towards Transparent Intrusion Detection: A Coherence-Based Framework in Explainable AI Integrating Large Language Models**
Areej Alnahdi (University of Massachusetts Lowell) and Sashank Narain (University of Massachusetts Lowell)

**PrivComp-KG: Leveraging KG and LLM for Compliance Verification**
Leon Garza (The Univeristy of Texas at El Paso), Lavanya Elluri (Texas A&M University - Central Texas), Aritran Piplai (The Univeristy of Texas at El Paso), Anantaa Kotal (The Univeristy of Texas at El Paso), Deepti Gupta (Texas A&M University - Central Texas) and Anupam Joshi (University of Maryland Baltimore County)

**A Qualitative Study on Using ChatGPT for Software Security: Perception vs. Practicality**
M. Mehdi Kholoosi (The University of Adelaide), M. Ali Babar (The University of Adelaide) and Roland Croft (The University of Adelaide)

**Automated Consistency Analysis of LLMs**
Aditya Patwardhan (University at Stonybrook), Vivek Vaidya (Rutgers University) and Ashish Kundu (Head of Cybersecurity Research, Cisco Research)

**Bridging the Legal Divide: Contractual Enforceability and Acceptability in the AI-Driven Automated Conversion of Smart Legal Contracts**
Shriyaa Balaji (University of North Texas), Ram Dantu (University of North Texas), Kritagya Upadhyay (Middle Tennessee State University) and Thomas McCullough (University of North Texas)

## CogMI Invited Research/Vision Session 2: Systems, Applications, and AI Performance

10:00 AM – 12:00 PM

Room: Gaston

Session Chair: Keke Chen (UMBC, USA)

**Data-Driven Vulnerable Community Identification During Compound Disasters**
Jainil Anilkumar Patel (University of Missouri–Kansas City), Mohammadreza Akbari Lor (University of Missouri–Kansas City), Shu-Ching Chen (University of Missouri–Kansas City), Mei-Ling Shyu (University of Missouri–Kansas City) and Steven Luis (Florida International University)

**A Perspective on Decentralizing AI**
Abhishek Singh (Massachusetts Institute of Technology), Charles Lu (Massachusetts Institute of Technology), Gauri Gupta (Massachusetts Institute of Technology), Ayush Chopra (Massachusetts Institute of Technology), Jonas Blanc (Massachusetts Institute of Technology), Tzofi Klinghoffer (Massachusetts Institute of Technology), Kushagra Tiwary (Massachusetts Institute of Technology) and Ramesh Raskar (Massachusetts Institute of Technology)

**Explainability and Interpretability of Large Language Model Predictions**
Upendra Sharma (IBM T. J. Watson Research Center) and Sriya Ayachitula (Ardsley High School)

**Open Human-Robot Collaboration Systems (OHRCS): A Research Perspective**
Prasanth Sengadu Suresh (University of Georgia), Diego Romeres (Mitsubishi Electric Research Laboratories), Prashant Doshi (University of Georgia) and Siddarth Jain (Mitsubishi Electric Research Laboratories)

**A Study of Response Time Instability of Microservices at High Resource Utilization in the Cloud**
Qingyang Wang (Louisiana State University), Xuhang Gu (Louisiana State University) and Calton Pu (Georgia Institute of Technology)

**A Graph-based Approach to Human Activity Recognition**
Thomas Peroutka (TU Wien), Ilir Murturi (TU Wien), Praveen Kumar Donta (Stockholm University) and Schahram Dustdar (TU Wien)

## CIC Session 2: AI-driven Systems, Security and Computing

10:00 AM – 12:00 PM

Room:  Ellington

Session Chair: Barbara Carminati (University of Insubria, Italy)

**A Survey on Privacy Attacks Against Digital Twin Systems in AI-Robotics**
Ivan A. Fernandez (Mississippi State University), Subash Neupane (Mississippi State University), Trisha Chakraborty (Mississippi State University), Shaswata Mitra (Mississippi State University), Sudip Mittal (Mississippi State University), Nisha Pillai (Mississippi State University), Jingdao Chen (Mississippi State University) and Shahram Rahimi (Mississippi State University)

**Polarization Detection on Social Networks: dual contrastive objectives for Self-supervision**
Hang Cui (University of Illinois,Urbana Champaign) and Tarek Abdelzaher (University of Illinois at Urbana-Champaign)

**Graph Neural Networks with Node Connectivity Strength for Node Classification**
Jingdong Liu (Shanghai Jiao Tong University), Tao Fang (Shanghai Jiao Tong University) and Hong Huo (Shanghai Jiao Tong University)

**Enhancing Explainability and Trustworthiness of Intrusion Detection Systems Using Competitive Learning**
Jesse Ables (Mississippi State University), Thomas Kirby (Mississippi State University), William Anderson (Mississippi State University), Sudip Mittal (Mississippi State University), Ioana Banicescu (Mississippi State University), Shahram Rahimi (Mississippi State University), Maria Seale (U.S Army Engineer Research and Development Center), Thomas Arnold (U.S Army Engineer Research and Development Center) and Joseph Jabour (U.S Army Engineer Research and Development Center)

**Utilizing Graph Neural Networks to Detect Abnormal Driving Patterns in Vehicular Networks**
Harir Razzazi (University Of Missouri - Kansas City), Farid Nait-Abdesselam (University Of Missouri - Kansas City) and Maroua Nouiri (University of Nantes)

**RFPG: Question-Answering from Low-Resource Language (Arabic) Texts using Factually Aware RAG**
Mitha Alshammary (The University of Texas at Dallas), Md Nahiyan Uddin (The University of Texas at Dallas) and Latifur Khan (The University of Texas at Dallas)

## TPS Invited Research/Vision 2: AI, Quantum Computing, and Cybersecurity

10:00 AM – 12:00 PM
Room: Whitman
Session Chair: Amir Masoumzadeh (SUNY-Albany, US)

**Counter Denial of Service for Next-Generation Networks within the Artificial Intelligence and Post-Quantum Era**
Saleh Darzi (University of South Florida) and Attila A Yavuz (University of South Florida)

**Federated Learning in Practice: Reflections and Projection**
Katharine Daly (Google), Hubert Eichner (Google), Adria Gascon (Google), Peter Kairouz (Google), H Brendan McMahan (Google), Daniel Ramage (Google) and Zheng Xu (Google)

**Privacy in Practice: Research Challenges in the Deployment of Privacy-Preserving ML**
Stacey Truex (Denison University) and Margaret Malan (Denison University)

**ZCube: A Zero-Trust, Zero-Knowledge, and Zero-Memory Platform for Privacy and yet Secured Access**
Vinh Quach (University of North Texas), Ram Dantu (University of North Texas), Sirisha Talapuru (University of North Texas), Shakila Zaman (University of North Texas) and Apurba Pokharel (University of North Texas)

**Harnessing Deep Learning for Fault Detection in Industry 4.0: A Multimodal Approach**
Jialie Shen (City St George’s, University of London, UK), Marie Morrison (University of Bristol, Bristol, UK), Haiyan Miao (University of Huddersfield, Huddersfield, UK) and Fengshou Gu (University of Huddersfield, Huddersfield, UK)

**The Intersection of Quantum Computing, AI, and Cybersecurity: Challenges and Opportunities**
Danda B Rawat (Howard University) and Chandra Bajracharya (University of Maryland Global Campus)

## Lunch Break (provided by conference) and Panel Session (Room: Logan Ballroom)

12:00 PM – 02:00 PM

**Panel Name: Student Mentoring Panel**

**Panelists**: Huan Liu (Arizona State University, US), Indrakshi Ray (Colorado State University, US), Stacey Truex (Denison University, US), Peter Kairouz (Google, USA), Ambareen Siraj (SFS/SaTC Program, NSF, US*)*

**Moderator**: *W*enqi Wei (Fordham University, US)

## Keynote 5 (Room: Logan Ballroom)

02:00 PM – 03:00 PM

**Roshan Thapliya,** Corporate Officer, Chief Digital Transformation Officer and General Manager, TDK Corporation, Tokyo, Japan

Title: Transforming Society: TDK's Vision Accelerated by Digital Transformation

Chair: James Joshi (University of Pittsburgh, US)

### Coffee Break (15 min)

## TPS Session 3: Privacy and Security in AI/ML

03:15 PM – 05:15 PM

Room: Logan Ballroom

Session Chair: Dipankar Dasgupta (University of Memphis, US)

**Dynamic Black-box Backdoor Attacks on IoT Sensory Data**
Ajesh Koyatan Chathoth (University of Pittsburgh) and Stephen Lee (University of Pittsburgh)

**Resilient Federated Learning Using Trimmed-Clipping Aggregation**
Chandreyee Bhowmick (Vanderbilt University) and Xenofon Koutsoukos (Vanderbilt University)

**Noise as a Double-Edged Sword: Reinforcement Learning Exploits Randomized Defenses in Neural Networks**
Steve Bakos (Ontario Tech University), Pooria Madani (Ontario Tech University) and Heidar Davoudi (Ontario Tech University)

**Preserving Privacy During Reinforcement Learning With AI Feedback**
David Gao (Vanderbilt University), Ian Miller (Vanderbilt University), Ali Allami (Vanderbilt University) and Dan Lin (Vanderbilt University)

**Towards Assessing Integrated Differential Privacy and Fairness Mechanisms in Supervised Learning**
Maryam Aldairi (University of Pittsburgh) and James Joshi (University of Pittsburgh)

**MOFHEI: Model Optimizing Framework for Fast and Efficient Homomorphically Encrypted Neural Network Inference**
Parsa Ghazvinian (Georgia State University), Robert Podschwadt (Old Dominion University), Prajwal Panzade (Georgia State University), Mohammad H. Rafiei (Georgia State University) and Daniel Takabi (Old Dominion University.)

## CogMI Session 2: AI-driven decision-making and human-centered systems

03:15 PM – 05:15 PM

Room: Gaston

Session Chair: Keke Chen (UMBC, US)

**Trust and Collaboration Testing in Controlled Human-Robot Environments**
John Frericks (University of Georgia), Brandon Kang (University of Georgia), Neal Outland (University of Georgia), Prashant Doshi (University of Georgia), Kyle Johnsen (University of Georgia) and Aaron Schecter (University of Georgia)

**Sense-making and knowledge construction via constructivist learning paradigm**
Jianyong Xue (Université Paris-Saclay, CEA, France), Raphaël Lallement (Université Paris-Saclay, CEA, France) and Matteo Morelli (Université Paris-Saclay, CEA, France)

**Explainable Anomaly Detection: Counterfactual driven What-If Analysis**
Logan Cummins (Mississippi State University), Alexander Sommers (Mississippi State University), Sudip Mittal (Mississippi State University), Shahram Rahimi (Mississippi State University), Maria Seale (US Department of Defense), Joseph Jabour (US Department of Defense) and Thomas Arnold (US Department of Defense)

**Fair Evaluator: An Adversarial Debiasing-based Deep Learning Framework in Student Admissions**
Amisha Priyadarshini (University of California Irvine) and Sergio Gago-Masague (University of California Irvine)

**Advancing Mental Health Pre-Screening: A New Custom GPT for Psychological Distress Assessment**
Jinwen Tang (University of Missouri) and Yi Shang (University of Missouri)

**Multi-agent Reinforcement Learning for Dynamic Dispatching in Material Handling Systems**
Xian Yeow Lee (Hitachi America Ltd.), Haiyan Wang (Hitachi America Ltd.), Daisuke Katsumata (Hitachi America Ltd.), Takaharu Matsui (Hitachi America Ltd.) and Chetan Gupta (Hitachi America Ltd.)

## CogMI Session 3: AI and Language Models for human-centered systems

03:15 PM – 05:15 PM

Room: Ellington

Session Chair: Kim Hemmings-Jarrett (PSU, US)

**Optimizing Human-Robot Collaboration in Industry 5.0: A Comparative Study of Communication Mediums and Their Impact on Worker Well-being and Productivity**

Bsher Karbouj (Technical University Berlin), Per Sören Tobias Schuster (Technical University Berlin), Moritz Blumhagen (Technical University Berlin) and Jörg Krüger (Fraunhofer Institute IPK)

**Neural Bezier Interpolation with Manifold Learning for Reliable Vessel Trajectory Prediction**
Gawon Lee (Major in Industrial Data Science & Engineering, Department of Industrial Engineering, Pusan National University), Dohee Kim (Safe & Clean Supply Chain Research Center, Pusan National University), Segil Park (Korea Research Institute of Ships and Ocean Engineering (KRISO), Daejeon City, South Korea), Sunghyun Sim (Major in Industrial Management and Big Data Engineering, Dong-Eui University), Ling Liu (College of Computing, Georgia Institute of Technology) and Hyerim Bae (Department of Data Science, Graduate School of Data Science, Pusan National University)

**Catching Chameleons: Detecting Evolving Disinformation Generated using Large Language Models**
Bohan Jiang (Arizona State University), Chengshuai Zhao (Arizona State University), Zhen Tan (Arizona

State University) and Huan Liu (Arizona State University)

**Decoding Linguistic Nuances in Mental Health Text Classification Using Expressive Narrative Stories**
Jinwen Tang (University of Missouri), Qiming Guo (Texas A\&M University-Corpus Christi), Yunxin Zhao (University of Missouri) and Yi Shang (University of Missouri)

**Cognitive Chunks, Neural Engrams and Natural Concepts: Bridging the Gap between Connectionism and Symbolism**
Dmitry Bennett (London School of Economics) and Fernand Gobet (London School of Economics)

**Evolving Cognitive Models: A Novel Approach to Verbal Learning**
Dmitry Bennett (London School of Economics), Noman Javed (London School of Economics), Laura Bartlett (London School of Economics), Peter Lane (University of Hertfordshire) and Fernand Gobet (London School of Economics)

## TPS Invited Research/Vision 3: AI Security, Privacy, and Healthcare

03:15 PM – 05:15 PM
Room: Whitman
Session Chair: Indrakshi Ray (CSU, US)

**LLM-Sentry: A Model-Agnostic Human-in-the-Loop Framework for Securing Large Language Models**
Saquib Irtiza (University of Texas at Dallas), Khandakar Ashrafi Akbar (University of Texas at Dallas), Arowa Yasmeen (University of Texas at Dallas), Latifur Khan (University of Texas at Dallas), Ovidiu Daescu (University of Texas at Dallas) and Bhavani Thuraisingham (University of Texas at Dallas)

**PrivacySphere: towards a Framework for Privacy-Preserving Smart Spaces with the following co-authors**
Habiba Farrukh (University of California, Irvine), Nada Lajouji (University of California, Irvine), Sharad Mehrotra (University of California, Irvine), Faisal Nawab (University of California, Irvine), Shantanu Sharma (New Jersey Institute of Technology), Nalini Venkatasubramanian (University of California, Irvine) and Roberto Yus (University of Maryland, Baltimore County)

**Patient-Centered and Practical Privacy to Support AI for Healthcare**
Ruixuan Liu (Emory University), Hong Kyu Lee (Emory University), Sivasubramanium V Bhavani (Emory University), Xiaoqian Jiang (UTHealth at Houston), Lucila Ohno-Machado (Yale University) and Li Xiong (Emory University)

**Enabling Learning Health Care systems using advances in Privacy-Preserving Federated Learning**
Zilinghan Li (Argonne National Laboratory), Kibaek Kim (Argonne National Laboratory), Tarak Nandi (Argonne National Laboratory) and Ravi K. Madduri (Argonne National Laboratory)

**Towards Privacy-Preserving and Secure Machine Unlearning: Taxonomy, Challenges and Research Directions**
Liou Tang (University of Pittsburgh) and James Joshi (University of Pittsburgh)

## Banquet Dinner (provided by the conference)

06:00 PM – 09:00 PM

# IEEE 2024 CIC/CogMI/TPS Joint Conferences
# Day 3: Wednesday, October 30, 2024

## Registration & Continental Breakfast (provided by conference)

7:15 AM - 8:00 AM

## TPS Session 4: Malware and Threat Detection

08:00 AM – 10:00 AM

Room: Logan Ballroom

Session Chair: Pooria Madani (Ontario Tech University, Canada)

**Resiliency Graphs: Modelling the Interplay between Cyber Attacks and System Failures through AI Planning**
Shadaab Kawnain Bashir (Colorado State University), Rakesh Podder (Colorado State University), Sarath Sreedharan (Colorado State University), Indrakshi Ray (Colorado State University) and Indrajit Ray (Colorado State University)

**SR2ACM: Security Requirements to Access Control Model: A Methodological Approach to Translating Natural Language Security Specifications into Structured Access Control Models**
Saja Alqurashi (Colorado State University), Indrakshi Ray (Colorado State University), Mahmoud Abdelgawad (Colorado State University) and Hossein Shirazi (San Diego State University)

**Fine-Tuning LLMs for Code Mutation: A New Era of Cyber Threats**
Mohammad Setak (Ontario Tech University) and Pooria Madani (Ontario Tech University)

**HAL 9000: a Risk Manager for ITSs**
Tadeu Freitas (Faculty of Science of the University of Porto), Carlos Novo (Faculty of Science of the University of Porto), João Soares (Faculty of Science of the University of Porto), Manuel Correia (Faculty of Science of the University of Porto), Inês Dutra (Faculty of Science of the University of Porto and CINTESIS@RISE), Behnam Shariati (University of Maryland Baltimore County) and Rolando Martins (SafeHelm, lda)

**Discovery of Evolving Relationships of Software Vulnerabilities**
Hailey Sparks (College of Charleston) and Krishnendu Ghosh (College of Charleston)

**Leveraging Multimodal Retrieval-Augmented Generation for Cyber Attack Detection in Transit Systems**
Yuchen Cai (The University of Texas at Dallas), Muhaimin Bin Munir (The University of Texas at Dallas), Bhavani Thuraisingham (The University of Texas at Dallas) and Latifur Khan (The University of Texas at Dallas)

## CogMI Session 4: AI-driven modeling and analysis for behavioral and network systems

08:00 AM – 10:00 AM

Room: Ellington

Session Chair: Yanzhao Wu (FIU, USA)

**Enhanced Model Robustness by Integrated Local and Global Processing**
Longwei Wang (University of South Dakota), Aashish Ghimire (University of South Dakota) and Kc

Santosh (University of South Dakota)

**Dynamic Network Analysis of Propaganda Networks Using Meta-Network Modeling and Community Detection Algorithms**
Abdullah Melhem (Augusta University), Zain Halloush (Augusta University) and Ahmed Aleroud (Augusta University)

**EMDA-Net: Earth Mover's Distance (EMD) influenced Attention-aided Neural Network for Medical Image Classification**
Surya Majumder (Heritage Institute of Technology), Kushaj Mallick (Jadavpur University), Wrick Pal (Jadavpur University), Somenath Chakraborty (Leonard C. Nelson College of Engineering and Sciences) and Ram Sarkar (Jadavpur University)

**How We Browse: Measurement and Analysis of Browsing Behavior**
Yuliia Lut (Unaffiliated researcher), Michael Wang (Unaffiliated researcher), Elissa M. Redmiles (Georgetown University) and Rachel Cummings (Columbia University)

**Investigating the Impact of Randomness on Reproducibility in Computer Vision: A Study on Applications in Civil Engineering and Medicine**
Bahadır Eryılmaz (Institute for AI in Medicine, University Hospital Essen), Osman Alperen Koras (Institute for AI in Medicine, University Hospital Essen), Jörg Schlötterer (University of Marburg) and Christin Seifert (University of Marburg)

## Coffee Break

## Panel 2 (Room: Logan Ballroom)

10:15 AM – 12:15 PM

Panel Title: **Driving Innovations in Emerging Technologies: R&D Priorities and Funding Landscape**

**Panelists**: Jennifer Roberts (Director, Resilient Systems, ARPA-H, USA), Heidi Sofia (Deputy Director, NCBI-NIH, USA), Elham Tabassi (Associate Director of Emerging Technology, NIST, USA), Cliff Wang, (Program Director, SaTC Program, NSF, USA), Dr. Craig Schlenoff (Director, NITRD + AD of Networking and IT at White House OSTP)

**Moderators**: James Joshi, University of Pittsburgh, USA and Huan Liu, Arizona State University, USA

## Lunch Break

12:15 PM – 01:15 PM

## TPS Session 5: Access Control and Security Models

01:15 AM – 03:00 PM

Room: Logan Ballroom

Session Chair: Wenqi Wei (Fordham University, USA)

**BobGAT: Towards Inferring Software Bill of Behavior with Pre-Trained Graph Attention Networks**
Justin Allen (Lawrence Livermore National Lab) and Geoff Sanders (Lawrence Livermore National Lab)

**Translating Natural Language Specifications into Access Control Policies by Leveraging Large Language Models**
Sherifdeen Lawal (Institute for Cyber Security, University of Texas at San Antonio, Texas), Xingmeng Zhao (Department of Information Systems and Cyber Security, University of Texas at San Antonio, Texas), Anthony Rios (Department of Information Systems and Cyber Security, University of Texas at San Antonio, Texas), Ram Krishnan (Department of Electrical & Computer Engineering, University of Texas

at San Antonio, Texas) and David Ferraiolo (National Institute of Standards and Technology, Gaithersburg, Maryland.)

**Constraints Visualization and Specification for Activity-centric Access Control**
Tanjila Mawla (Tennessee Tech University) and Maanak Gupta (Tennessee Tech University)

**Fast and Post-Quantum Authentication for Real-time Next Generation Networks with Bloom Filter**
Kiarash Sedghighadikolaei (University of South Florida) and Attila A Yavuz (University of South Florida)

**Secure Cross-Chain Provenance for Digital Forensics Collaboration**
Asma Jodeiri Akbarfam (Augusta University), Gokila Dorai (Augusta University) and Hoda Maleki (Augusta University)

**Genesis of Cyber Threats: Towards Malware-based Advanced Persistent Threat (APT) Attribution**
Nanda Rani (Indian Institute of Technology Kanpur), Bikash Saha (Indian Institute of Technology Kanpur), Ravi Kumar (C3iHub, IIT Kanpur) and Sandeep Kumar Shukla (Indian Institute of Technology Kanpur)

## Tutorial: Tutorial: Computational Scientific Discovery in Cognitive Science

1:15 PM – 3:00 PM
Room: Whitman
Tutorial Session Chair: Fernand Gobet (UK)

## Panel 3 (Room: Logan Ballroom)

3:00 pm -5:00 pm
Panel Title: **AI vs AI: The Inevitable Next Cyber Frontier**
**Panelists**: Karl Aberer, (EPFL, Switzerland), Elena Ferrari (University of Insubria, Italy), Anupam Joshi (UMBC, USA), Calton Pu (Georgia Tech, USA), Peter Kairouz (Google, USA)
**Moderator:** James Joshi (University of Pittsburgh, USA)

## Closing Remarks

5:00pm – 5:15pm
Room: Logan Ballroom

# Workshop Programs

# Workshop LLM CyberSec Agenda (Oct 28)

## Room: Deacon

## Keynote

11:00 AM – 11:30 AM

**Ali Babar,** Professor, University of Adelaide, Australia
Title: Evaluation of Using Large Language Models for Software Security: Learning from Analyzing a Few Cases

## Paper Session 1

11:30 AM – 12:10 PM

**Forensic Analysis of Indirect Prompt Injection Attacks on LLM Agents**
Maxim Chernyshev (Deakin University, Australia), Zubair Baig (Deakin University, Australia), and Robin Doss (Deakin University, Australia)

**Pitfalls of Generic Large Language Models (GLLMs) from Reliability and Security Perspectives**
Dipankar Dasgupta (The University of Memphis, USA) and Arunava Roy (The University of Memphis, USA)

## Paper Session 2

4:45 PM – 5:45 PM

**Large Language Models for Hardware Security**
Hammond Pearce (University of New South Wales, Australia) and BenjaminTan (University of Calgary, Canada)

**Secure Lightweight Computation for Federated N-Gram Language Models**
Tho Thi Ngoc Le (HUTECH University, Vietnam) and Tran Viet Xuan Phuong (University of Arkansas at Little Rock, USA)

**Probing Robustness of In-context Learning in LLM Classification Predictions Under Label Noise**
Sriya Ayachitula (Ardsley School, USA), Chinmay Kundu (KIIT University, India), and Birendra Mishra (University of California, Riverside, USA)

# Workshop Inclusive AI for Cybersecurity Agenda (Oct 28)

## Room: Whitman

## Keynote

11:00 AM – 11:35 AM

**TBD**

## Breakout Groups

11:35 AM – 12:20 PM

**Human factors behind vulnerabilities of AI tools for Cybersecurity**

## Paper Session 1

4:45 PM – 6:05 PM

**Design Challenges for Scam Prevention Tools to Protect Neurodiverse and Older Adult Populations** Pragathi Tummala (George Mason University), Hannah Choi (George Mason University), Anuridhi Gupta (George Mason University), Tomas A Lapnas (George Mason University), Yoo Sun Chung (George Mason University), Matthew Peterson (George Mason University), Geraldine G Walther (George Mason University), Hemant Purohit (George Mason University)

**Towards Inclusive Cybersecurity: Protecting the Vulnerable with Social Cyber Vulnerability Metrics** Shutonu Mitra (Virginia Tech), Qi Zhang (Virginia Tech), Chen-Wei Chang (Virginia Tech), Hossein Salemi (George Mason University), Hemant Purohit (George Mason University), Fengxiu Zhang (George Mason University), Michin Hong (Indiana University), Chang-Tien Lu (Virginia Tech), Jin-Hee Cho (Virginia Tech)

**A Blockchain-Enabled Approach to Cross-Border Compliance and Trust** Vikram Kulothungan (Capitol Technology University)

**Mind the Inclusion Gap: A Critical Review of Accessibility in Anti-Counterfeiting Technologies** Salem Abdul-Baki (George Mason University), Krishna Purohit (George Mason University), Hemant Purohit (George Mason University)

# Workshop QUILLS (Oct 29)

## Room: Deacon

## Keynote (Main Room)

8:50 AM – 9:50 AM

**The National Science Foundation's Role in the Future of AI**
Michael L. Littman (NSF)

## Session 1 Quantum Computing & Algorithms (Venue: Deacon)

10:00 AM – 12:00 PM
Session Chair: Junyu Liu (U. Pittsburgh)

**Randomized Benchmarking of Local Zeroth-Order Optimizers for Variational Quantum Systems**
Lucas Tecot (U. California Los Angeles), Cho-Jui Hsieh (U. California Los Angeles)

**Pragmatic Obfuscation of Factoring in Hamiltonian Simulation and Ground State Estimation**
Dhruv Gopalakrishnan (U. Waterloo), Michele Mosca (U. Waterloo)

**Exploration of Attacks on the HHL Quantum Algorithm**
Yizhuo Tan (Yale U.), Hrvoje Kukina (TU Wien), Jakub Szefer (Yale U.)

**Synergizing Error Suppression, Mitigation and Correction for Fault-Tolerant Quantum Computing**
Yanzhang Zhu (), Siyuan Niu (), Di Wu (U. Central Florida)

## Session 2 Panel on Quantum Cybersecurity: Challenges & Opportunities (Venue: Deacon)

2:00 PM – 3:00 PM

(Moderator: Kaushik Seshadreesan, University of Pittsburgh, USA)
Panel Experts: Michele Mosca (U. Waterloo), Junyu Liu (U. Pittsburgh), Eneet Kaur (Cisco Quantum Lab), Di Wu (U. Central Florida), Donna Dodson (EvolutionQ)

## Session 3 Quantum Services with Efficiency and Privacy (Venue: Deacon)

3:15 PM – 5:15 PM
Session Chair: Lucas Tecot (U. California, Los Angeles)

**Simulation of Quantum Homomorphic Encryption: Demonstration and Analysis**
Sohrab Ganjian (U. Ottawa), Connor Paddock (U. Ottawa), Anne Broadbent (U. Ottawa)

**Enhancing Quantum Security over Federated Learning via Post-Quantum Cryptography**
Pingzhi Li (UNC-Chapel Hill), Tianlong Chen (UNC-Chapel Hill), Junyu Liu (U. Pittsburgh)

**Network Operations Scheduling for Distributed Quantum Computing**
Nitish Chandra (U. Pittsburgh), Eneet Kaur (Cisco Quantum Lab), Kaushik Seshadreesan (U. Pittsburgh)

**Entangling Intelligence: AI-Quantum Crossovers and Perspectives**
Zhuo Chen (MIT), Di Luo (MIT)

**Towards efficient and secure quantum-classical communication networks**

Pei Zeng (U. Chicago), Debayan Bandyopadhyay (), Jose A. Mendez (), Nolan Bitner (), Alexander Kolar (), Michael T. Solomon (), F. Joseph Heremans (), David D. Awschalom (U. Chicago), Liang Jiang (U. Chicago), and Junyu Liu (U. Pittsburgh)

# Workshop Equitable and Inclusive Computing (EIC) (Oct 30)

## Room: Whitman

### VR warm up activities

**8:00 AM – 8:50 AM**

### Introduction & Welcome

- Opening remarks and introduction to the workshop.

**What is EIC?**

- Overview of Equitable and Inclusive Computing.
- Discussion on what we want our community to focus on or look like.

### Invited Speakers-Panel Discussion

**Lindsay Wood**
Director of Online Learning & Information Technology (OIT)

**Dr. Aniete Andy**
Professor of Electrical Engineering & Computer Science. Howard University

**Jamie Ofalt**
Co-Owner // Brand Strategist // Content Creator

**Dr. Sarah “Scout” Sinclair Brody**
Security Lead, Meta Reality Labs Trust

**8:50AM- 8:55 AM**

### VR and Networking Break

**8:55 AM - 9:55 AM**

## Session 1: EIC Session

**Conceptualizing the Paradox of Immersive Technologies in SIDS: Bridging the Digital Divide and Environmental Trade-offs in Climate Action**
Glenville Mcleod and Howard Reid

**Bridging NextG Network Connectivity Induced Digital Divide with Sustainable ICT**
Kuheli Sai and David Tipper,

Virtual Reality for Stress Management in University Students
**Stefani Abreu and Terri Stiles**

**9:55 PM - 10:00 AM**

## Closing Remarks

# Workshop SR-CIST Agenda (Oct 30)

## Room: Gaston

## Panel: Industrial Internet of Things (IIoT) Security

8:30 AM – 10:00 AM

**Panelists:**
**Dimitrios Georgakopoulos,** Director of Swinburne's key IoT Lab
**Henry Haswell**, Southwest Research Institute
**Joseph Slowik**, MITRE Corporation
**Matthew Rogers,** Cybersecurity and Infrastructure Security Agency (CISA)

**Moderator:**
**Mai Abdelhakim**, University of Pittsburgh

## Paper Session 1: CPS Security & Resiliency

10:15 AM – 12:15 PM
Henry Haswell, Southwest Research Institute

**Organizational Influence on Supply Chain for Digital Energy Infrastructure: Business Models, and Policy Landscape**
Gabriel Weaver (INL), Megan Culler (INL) and Emma Stewart (INL)

**Development of a Cyber-Physical Model and Emulation of an Oil and Gas Compressor Station for Cybersecurity Research and Development**,
Adam J. Beauchaine (Sandia National Laboratories), Titus A. Gray (Sandia National Laboratories), Andrew S. Hahn (Sandia National Laboratories), Lee T. Maccarone (Sandia National Laboratories), and Scott T. Bowman (Idaho National Laboratory)

**On the Application of Cyber-Informed Engineering**,
Benjamin Lampe (Idaho National Laboratory)

**Formal Verification of a Nuclear Plant Thermal Dispatch Operation Using System Decomposition**
Abhimanyu Kapuria (University of Pittsburgh) and Daniel Cole (University of Pittsburgh)

## Paper Session 2: SR- CIST Session 2: OT and Space Systems Security

1:15 PM – 3:00 PM
Session Chair: Benjamin Lampe, (Idaho National Laboratory)

**Statistical Methods for Developing Cybersecurity Response Thresholds for Operational Technology Systems Using Historical Data**
Connor Grady (Sandia National Naboratories), Shaw X. Wen (Idaho National Laboratory), Lee T Maccarone (Sandia National Naboratories), Scott T. Bowman (Idaho National Laboratory)

**Defensive Priorities in Securing Space-Based Infrastructure Dependencies**
Joe Slowik (The MITRE Corporation)

**Advancing Spacecraft Security Through Anomaly Detection**
Patrick Saenz (Southwest Research Institute), Nathan Wiatrek (Southwest Research Institute), Kisa Burnett (Southwest Research Institute), Szu-Li Lin (Southwest Research Institute) and Samantha Liu (Southwest Research Institute)

**Provably Secure and Optimal Inter-Satellite Link Authentication for Low Orbit Satellites**
Kerry Farrea (Deakin University), Zubair Baig (Deakin University), Robin Doss (Deakin University) and Dongxi Liu (Data61)

## The Third IEEE International Workshop on Assured Autonomy, Artificial Intelligence and Machine Learning (WAAM 2024), October 30, 2024

### Room: Deacon

The Third IEEE International Workshop on Workshop on Assured Autonomy, Artificial Intelligence and Machine Learning (WAAM 2024), which is part of The Sixth IEEE International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications (http://www.sis.pitt.edu/lersais/conference/tps/2024/) to be held from October 30 at the Darcy Hotel in the Washington DC. The theme of this year's workshop is **"Security and AI/ML"**

### Sessions

**Panel 1**: Security Threats to AI and ML Systems [Moderator: Phil Laplante, NIST], panel members TBD

**Panel 2**: Identifying and managing risks in public systems [Moderator: Joanna DeFranco, Penn State], panel members TBD

### Break

**Panel 3:** Identifying and managing risks in government systems [Moderator: Rick Kuhn, NIST], panel members TBD

### Lunch

**Panel 4:** AI and DevSecOps [Moderator: Tracy Bannon, MITRE], panel members TBD

**Panel 5:** Societal Implications: Awareness, Education, Training and Certification [Moderator M.S.

Raunak, NIST], panel members TBD

### Break

**Panel 6:** Industry-Government perspective (joint with TPS Conference) , panel members TBD