IEEE 2023 CIC/COGMI/TPS JOINT CONFERENCES

CONFERENCE PROGRAM

ATLANTA, GEORGIA, UNITED STATES OF AMERICA
NOVEMBER 1-3, 2023

VERSION
NOV 1

Useful Resources

Conference Website
- CIC: http://www.sis.pitt.edu/lersais/conference/cic/2023/
- TPS: http://www.sis.pitt.edu/lersais/conference/tps/2023/
- CogMI: http://www.sis.pitt.edu/lersais/conference/cogmi/2023/

Overview Day 1: Wednesday, Nov. 1, 2023

7:15 AM - 8:20 AM	Breakfast (provided by conference)				
8:30 AM - 9:30 AM	**Welcome and Opening Remarks** **M. Brian Blake, President of Georgia State University** (Session Chair: James Joshi, *University of Pittsburgh, USA*) (Main Room - Chastain Ballroom)				
09:45 AM – 10:45 AM	Keynote 1 (Main Room - Chastain Ballroom) **Who Benefits from the Data Economy?** **Alessandro Acquisti,** *Carnegie Mellon University, USA* (Chair: Paolo Boldi, *University of Milano, Italy*)				
10:45 AM – 11:00 AM	Break				
11:00 AM – 12:00 PM	Keynote 2 (Main Room - Chastain Ballroom) **Large Foundational Model Is a Blessing to Natural Language Understanding and Data Mining** **Jiawei Han**, *University of Illinois at Urbana-Champaign, USA* (Chair: Ling Liu, *Georgia Institute of Technology, USA*)				
12:00 PM – 02:00 PM	Mentoring Session (Main Room - Chastain Ballroom) **Balaji Palanisamy**, *University of Pittsburgh, USA* **Wenqi Wei**, *Fordham University, USA* **Panelists:** **Rachel Cummings**, *Columbia University, USA* **Murat Kantarcioglu**, *University of Texas at Dallas, USA* **Adrienne Raglin,** *Army Research Lab, USA* **Mei-Ling Shyu**, *University of Missouri-Kansas City, USA* **Jaideep Vaidya**, *Rutgers University, USA*				Launch Break
02:00 PM – 04:15 PM	**dDEI Workshop** (Main Room - Chastain Ballroom) **Kimberley Hemmings-Jarrett**, *Penn State University - Abington*	**TPS Session 1 – Vision: Trust and Privacy I** (Breakout 1 - Ponce De Leon) **Amir Masoumzadeh**, *University at Albany – SUNY, USA*	**CogMI Session 1 – Vision: AI Application and Ethics** (Breakout 2 - Roswell) **Jery Jialie Shen**, *City, University of London, UK*	**CIC Session 1 – Vision: Edge Computing, Architecture and Graphs analysis** (Breakout 3 - Brookhaven) **Mei-Ling Shyu**, *University of Missouri-Kansas City, USA*	**TPS Session 2 – Research: Security and Privacy in AI and IoT** (Breakout 4 - Peachtree) **Wenqi Wei**, *Fordham University, USA*
04:15 PM – 04:30 PM	Break				
04:30 PM – 06:30 PM	Panel 1 (Main Room - Chastain Ballroom) **Generative AI and Large Language Models: Research Impact and Open Challenges** **Moderator: Ling Liu,** *Georgia Institute of Technology, USA* **Panelists:** **Paolo Boldi**, *University of Milano, Italy* **Mark Riedl**, *Georgia Institute of Technology, USA* **Norman Sadeh**, *Carnegie Mellon University, USA* **Christin Seifert**, *University of Marburg, Germany*				

Overview Day 2: Thursday, Nov. 2, 2023

08:30 AM – 10:45 AM	**Tutorial Session** What Can We Really Expect from Foundation Models? Demystifying the Security and Privacy of These Trendy Models (Main Room - Chastain Ballroom) **Nathalie Baracaldo**, *IBM Research, USA*	**TPS Session 3 – Vision/Research: Trust and Privacy II** (Breakout 1 - Ponce De Leon) **Surya Nepal**, *CSIRO/Data61*, Australia *A*	**CogMI Session 2 – Research: Neural Networks, and AI Explainability** (Breakout 2 - Roswell) **Danda Rawat**, *Howard University, USA*	**CIC Session 2 – Vision/Research: Ransomware, Blockchain and AI** (Breakout 3 - Brookhaven) **Qingyang Wang**, *Louisiana State University-Baton Rouge, USA*	**WAAM Workshop** (Breakout 4 - Peachtree)
10:45 AM – 11:00 AM	Break				
11:00 AM – 12:00 PM	Keynote 3 (Main Room - Chastain Ballroom) **Can Federated Learning be Responsible?** **Ling Liu,** *Georgia Institute of Technology, USA* (Chair: Christen Seifert, *University of Marburg, Germany*)				
12:00 PM – 01:30 PM	Lunch Break (Lunch Provided)				
01:30 PM – 03:45 PM	**TPS Session 4 – Vision: AI/LLM Security and Explainability** (Main Room - Chastain Ballroom) **Li Xiong**, *Emory University, USA*	**TPS Session 5 – Research: Blockchain, Access Control and Privacy** (Breakout 1 - Ponce De Leon) **Wenbo He,** *McMaster University, Canada*	**CogMI Session 3 – Vision: AI, Computer Vision and Applications** (Breakout 2 - Roswell) **Paolo Boldi**, *University of Milano, Italy*	**CIC Session 3 – Vision: LLM, Multi-Modal Learning, Metaverse and Smart Infrastructure** (Breakout 3 - Brookhaven) **Arun Iyengar**, *Cisco Research, USA*	
03:45 PM – 04:00 PM	Break				
04:00 PM – 06:00 PM	Panel 2 (Main Room - Chastain Ballroom) **AI Impact and Challenges in Industry and Government** **Moderator: James Joshi**, *University of Pittsburgh, USA* **Panelists:** **Sandeep Gopisetty**, *IBM Research - Almaden, USA.* **Arun Iyengar**, *Cisco Research, USA* **Surya Nepal,** *CSIRO Data61, Australia* **Tao Zhang,** *NIST, USA*				
06:00 PM – 08:00 PM	**Banquet Dinner**				

Overview Day 3: Friday, Nov. 3, 2023

08:30 AM – 10:45 AM	**CIC/TPS Session 6 – Vision: Security and Trust in LLMs, IoT and Metaverse** (Main Room - Chastain Ballroom) **Balaji Palanisamy**, *University of Pittsburgh, USA*	**TPS Session 7 – Research: Security and Privacy** (Breakout 1 - Ponce De Leon) **Shamik Sural,** *IIT, Kharagpur, India*	**CogMI Session 4 – Research / Vision: AI and Machine Learning** (Breakout 2 - Roswell) **Indrakshi Ray,** *Colorado State University, USA*	**CogMI Session 5 – Research: AI and Applications** (Breakout 3 - Brookhaven) **Yanzhao Wu**, *Florida International University, USA*	**Industry Session** (Breakout 4 - Peachtree) **Indrajit Ray**, *Colorado State University, USA*
10:45 AM – 11:00 AM	Break				
11:00 AM – 12:00 PM	Keynote 4 (Main Room - Chastain Ballroom) **Advancing Technology, Innovation and Partnerships** **Erwin Gianchandani,** *National Science Foundation (NSF), USA* (Chair: James Joshi, *University of Pittsburgh, USA*)				
12:00 PM – 01:30 PM	Lunch Break				
01:30 PM – 03:30 PM	Panel 3 (Main Room - Chastain Ballroom) **Grand Challenges in Cyber Security and Privacy** **Moderator:** **James Joshi,** *University of Pittsburgh, USA* **Panelists:** **Elisa Bertino**, *Purdue University, USA* **Anupam Joshi,** *University of Maryland Baltimore County, USA* **Vladimir Kolesnikov,** *Georgia Institute of Technology, USA* **Elaine Shi,** *Carnegie Mellon University, USA*				
03:00 PM – 04:00 PM	Break				
04:00 PM – 05:00 PM	**Closing Remarks** (Main Room - Chastain Ballroom)				

IEEE 2023 CIC/CogMI/TPS Joint Conferences

Day 1: Wednesday, Nov. 1, 2023

Welcome and Opening Remarks

9:00 am – 9:45 am
All Participants and Chairs
Main Room - Chastain Ballroom

Opening Remarks from M. Brian Blake, President of Georgia State University

Session Chair: James Joshi*, University of Pittsburgh, USA*

Keynote 1

9:45 am – 10:45 am, Room: Main Room - Chastain Ballroom
Session Chair: **Paolo Boldi***, University of Milano, Italy*

Who Benefits from the Data Economy?

Alessandro Acquisti
Carnegie Mellon University, USA

Coffee Break (15 min)

Keynote 2

11:00 am – 12:00 am, Room: Main Room - Chastain Ballroom
Session Chair: Ling Liu, *Georgia Institute of Technology, USA*

Large Foundational Model Is a Blessing to Natural Language Understanding and Data Mining

Jiawei Han
University of Illinois at Urbana-Champaign, USA

Mentoring Session + Lunch Break

12:00 pm – 2:00 pm, Room: Main Room - Chastain Ballroom

Session Chairs: Balaji Palanisamy, University of Pittsburgh, USA and Wenqi Wei, Fordham University, USA

Panelists (Last Name Alphabetical)

- **Rachel Cummings,** Columbia University, USA
- **Murat Kantarcioglu,** University of Texas at Dallas, USA
- **Adrienne Raglin,** Army Research Lab, USA
- **Mei-Ling Shyu,** University of Missouri-Kansas City, USA
- **Jaideep Vaidya,** Rutgers University, USA

TPS Session 1 – Vision: Trust and Privacy I

02:00 pm – 4:15 pm, Room: Breakout 1 - Ponce De Leon
Session Chair: Amir Masoumzadeh, *University at Albany – SUNY, USA*

○ **Ensuring Trust in Genomics Research**
Erman Ayday(Case Western Reserve University, United States of America), Jaideep Vaidya(Rutgers University, United States of America), Xiaoqian Jiang(University of Texas - Health Houston, United States of America) and Amalio Telenti(Scripps Institute, United States of America)

○ **RAI4IoE: Responsible AI for Enabling the Internet of Energy**
Minhui Xue(CSIRO's Data61, Australia), Surya Nepal(CSIRO's Data61, Australia), Ling Liu (Georgia Institute of Technology, United States of America), Subbu Sethuvenkatraman(CSIRO's Energy, Australia), Xingliang Yuan(Monash University, Australia), Carsten Rudolph(Monash University, Australia), Ruoxi Sun (CSIRO's Data61, Australia) and Greg Eisenhauer(Georgia Institute of Technology, United States of America)

○ **Preserving Location Privacy in the Modern Era of Pervasive Environments**
Tyler Nicewarner(Vanderbilt University, United States of America), Alian Yu(Vanderbilt University, United States of America), Wei Jiang(Oracle Labs, United States of America) and Dan Lin(Vanderbilt University, United States of America)

○ **Centering Policy and Practice: Research Gaps around Usable Differential Privacy**
Jayshree Sarathy(Columbia University, United States of America) and Rachel Cummings (Columbia University, United States of America)

○ **Synthetic Information and Digital Twins for Pandemic Science: Challenges and Opportunities**
Galen Harrison(University of Virginia, United States of America), Przemyslaw Porebski(University of Virginia, United States of America), Mandy Wilson(University of Virginia, United States of America), Jiangzhuo Chen(University of Virginia, United States of America), Henning Mortveit(University of Virginia, United States of America), Parantapa Bhattacharya(University of Virginia, United States of America), Dawen Xie(University of Virginia, United States of America), Stefan Hoops(University of Virginia, United States of America), Anil Vullikanti(University of Virginia, United States of America), Li Xiong(Emory University, United States of America), Madhav Marathe(University of Virginia, United States of America)

○ **Supporting pandemic preparedness with Privacy Enhancing Technology**
Ruixuan Liu(Emory University, United States of America), Sepanta Zeighami(University of Southern California, United States of America), Haowen Lin(University of Southern California, United States of America), Cyrus Shahabi(University of Southern California, United States of America), Yang Cao(Hokkaido University, Japan), Shun Takagi(Kyoto University, Japan), Yoko Konishi(Kochi

University, Japan), Masatoshi Yoshikawa(Osaka Seikei University, Japan) and Li Xiong(Emory University, United States of America)

CogMI Session 1 – Vision: AI Application and Ethics

02:00 pm – 4:15 pm, Room: Breakout 2 - Roswell
Session Chair: Jerry Jialie Shen, *City, University of London, UK*

- **Artificial Intelligence for Climate Smart Forestry: A Forward-Looking Vision**
  Feng Luo(Clemson University, United States of America), Ling Liu(Georgia Institute of Technology, United States of America), Geoff Wang(Clemson University, United States of America), Vijay Kumar(University of Pennsylvania, United States of America) and Mark Ashton(Yale University , United States of America)

- **A novel approach to synthesize class labels in highly imbalanced large data**
  Robert Kennedy (Florida Atlantic University, United States of America) and Taghi Khoshgoftaar (Florida Atlantic University, United States of America)

- **Evolution of Knowledge in Social Media and Their Relationship to an Evolving Real World**
  Calton Pu (Georgia Institute of Technology, United States of America), Abhijit Suprem(Georgia Institute of Technology, United States of America), Aibek Musaev (Georgia Institute of Technology, United States of America), Joao Eduardo Ferreira (University of Sao Paulo, Brazil)

- **AI Ethics: A Vision Perspective**
  Christen Seifert (University of Marburg, Germany)

- **Location-Adaptive Generative Graph Augmentation for Fraud Detection**
  Lin Meng(Florida State University, United States of America), Xiaonan Zhang(Florida State University, United States of America), Jiawei Zhang(University of California, Davis, United States of America) and Philip S. Yu(University of Illinois, Chicago, United States of America)

CIC Session 1 – Vision: Edge Computing, Architecture and Graphs analysis

02:00 pm – 4:15 pm, Room: Breakout 3 - Brookhaven
Session Chair: Mei-Ling Shyu, *University of Missouri-Kansas City, USA*

- **The Emergence of Hypergraphs in Complex System Analysis**
  Paolo Boldi(University of Milan, Italy)

- **EMBARK: Memory bounded architectural improvement in CSR-CSC Sparse Matrix Multiplication**
  Shakya Jayakody(University of Central Florida, United States of America) and Jun Wang(University of Central Florida, United States of America)

- **Edge-Assisted Over-the-Air Automotive Software Updates**
  Arpan Bhattacharjee(University of Delaware, United States of America), Hamza Mahmood(University of Delaware, United States of America), Sidi Lu(William & Mary, United States of America), Nejib Ammar(Toyota InfoTech Lab, United States of America), Akila Ganlath(Toyota InfoTech Lab, United States of America) and Weisong Shi(University of Delaware, United States of America)

- **Online Allocation of Sensing and Computation in Large Graphs**
  Xinlin Li(University of California, Los Angeles, United States of America), Merve Karakas(University of California, Los Angeles, United States of America), Osama Hanna(University of California, Los Angeles, United States of America), Mehrdad Kiamari(University of Southern California, United States

of America), Jared Coleman(University of Southern California, United States of America), Christina Fragouli(University of California, Los Angeles, United States of America), Bhaskar Krishnamachari(University of Southern California, United States of America) and Gunjan Verma (Army Research Laboratory, United States of America)

- **RESONATE: Advancing Sustainability in IoT Networks Through Smart and Selective Data Streaming**
  Ragini Gupta(University of Illinois at Urbana-Champaign, United States of America), Klara Nahrstedt(University of Illinois at Urbana-Champaign, United States of America) and Claudiu Danilov(Boeing Research & Technology, United States of America)

TPS Session 2 – Research: Security and Privacy in AI and IoT

02:00 pm – 4:15 pm, Room: Breakout 4 - Peachtree
Session Chair: Wenqi Wei, Fordham University, USA

- **FUBA: Federated Uncovering of Backdoor Attacks for Heterogeneous Data**
  Fabiola Espinoza Castellon(CEA List, France), Deepika Singh(CEA List, France), Aurélien Mayoue (CEA List, France) and Cédric Gouy-Pailler(CEA List, France)

- **Learnable Image Transformations for Privacy Enhanced Deep Neural Networks**
  David Rodriguez(University of Texas at San Antonio, United States of America) and Ram Krishnan(University of Texas at San Antonio, United States of America)

- **Metamorphic Malware Evolution: The Potential and Peril of Large Language Models**
  Pooria Madani(Ontario Tech University, Canada)

- **A Privacy-Preserving Framework for Collaborative Machine Learning with Kernel methods**
  Anika Hannemann(University of Leipzig, Germany), Ali Burak Ünal(University of Tübingen, Germany), Arjhun Swaminathan(University of Tübingen, Germany), Erik Buchmann(University of Leipzig and ScaDS.AI, Germany) and Mete Akgün(University of Tübingen, Germany)

- **Mitigating Targeted Universal Adversarial Attacks on Time Series Power Quality Disturbances Models**
  Sultan Uddin Khan(North Carolina A&T State University, United States of America), Mohammed Mynuddin(North Carolina A&T State University, United States of America), Isaac Adom (North Carolina A&T State University, United States of America) and Mahmoud Nabil Mahmoud (North Carolina A&T State University, United States of America)

- **Resource-Efficient and Data Type-Aware Authentication Protocol for Internet of Things Systems**
  Cong Pu(Oklahoma State University, United States of America), Imtiaz Ahmed(Howard University, United States of America) and Sumit Chakravarty(Kennesaw State University, United States of America)

Coffee Break (15 min)

Panel 1

04:30 pm – 06:30 pm, Room: Main Room - Chastain Ballroom

Generative AI and Large Language Models: Research Impact and Open Challenges

Moderator: **Ling Liu**, Georgia Institute of Technology, USA

Panelists (Last Name Alphabetical)

- **Paolo Boldi,** University of Milano, Italy
- **Mark Riedl,** Georgia Institute of Technology, USA
- **Norman Sadeh,** Carnegie Mellon University, USA
- **Christin Seifert,** University of Marburg, Germany

IEEE 2023 CIC/CogMI/TPS Joint Conferences

Day 2: Thursday, Nov. 2, 2023

Tutorial

8:30 am – 10:45 am, Room: Main Room - Chastain Ballroom

What Can We Really Expect from Foundation Models? Demystifying the Security and Privacy of These Trendy Models

Nathalie Baracaldo
IBM Almaden Research Center, USA

TPS Session 3 – Vision/Research: Trust and Privacy II

8:30 am – 10:45 am, Room: Breakout 1 - Ponce De Leon
Session Chair: Surya Nepal, *CSIRO/Data61*, Australia

○ **Trust, Privacy and Security Aspects of Bias and Fairness in Machine Learning**
Asli Atabek(Koc University, Turkey), Egehan Eralp(Koc University, Turkey) and M. Emre Gursoy (Koc University, Turkey)

○ **Web 3.0 and the Ownership of Learning**

○ Sarah Flanery(Texas A&M University, United States of America), Christiana Chamon(Texas A&M University, United States of America), Srujan Kotikela(Texas A&M University - Commerce, United States of America) and Francis Quek(Texas A&M University, United States of America)

○ **ForensiBlock: A Provenance-Driven Blockchain Framework for Data Forensics and Auditability**
(Application Paper)
Asma Jodeiri Akbarfam(Augusta University, United States of America), Mahdieh Heidaripour(Augusta University, United States of America), Hoda Maleki (Augusta University, United States of America), Gokila Dorai (Augusta University, United States of America) and Gagan Agrawal (University of Georgia, United States of America)

○ **Seamless Asset Exchange in Interconnected Metaverses: Unraveling On-Chain Atomic Swap**
(Application Paper)
Shakila Zaman(University of North Texas, United States of America), Ram Dantu(University of North Texas, United States of America), Syed Badruddoja(University of North Texas, United States of America), Sirisha Talapuru(University of North Texas, United States of America) and Kritagya Upadhyay (University of North Texas, United States of America)

○ **Revisit Linear Transformation for Image Privacy in Machine Learning**
Zhiwei Xu(McMaster University, Canada), Yangdi Lu(McMaster University, Canada) and Wenbo He(McMaster University, Canada)

○ **Privacy-preserving Oriented Design for Multi-modality Models using Federated Learning**
Mohammed Alduniawi(Florida International University), Kemal Akkaya (Florida International University) and Ruimin Sun (Florida International University)

CogMI Session 2 – Research: Neural Networks, and AI Explainability

8:30 am – 10:45 am, Room: Breakout 2 - Roswell
Session Chair: Danda Rawat, *Howard University, USA*

- **Ensuring Trustworthy Neural Network Training via Blockchain**
  Edgar Navarro (San Diego State University, United States of America), Kyle J. Standing (Brigham Young University, United States of America), Gaby G. Dagher (Boise State University, United States of America) and Tim Andersen(Boise State University, United States of America)

- **A Cognitive Behavioral AI: Novel Conversational Memory Elements for Technical Understanding of Medical Deep Denoisers**
  Swati Rai(Indian Institute of Information Technology Vadodara, India), Jignesh S. Bhatt(Indian Institute of Information Technology Vadodara, India), Sarat Kumar Patra(National Institute of Technology Agartala, India) and Tanmay Ambadkar(The Pennsylvania State University, United States of America)

- **CLIMAX: An exploration of Classifier-Based Contrastive Explanations**
  Praharsh Nanavati(Indian Institute of Science Education & Research, India) and Ranjitha Prasad(Indraprastha Institute of Information Technology, India)

- **Feature Attribution Explanations for Spiking Neural Networks**
  Elisa Nguyen(University of Twente, Netherlands), Meike Nauta(University of Twente, Netherlands), Gwenn Englebienne(University of Twente, Netherlands) and Christin Seifert(University of Marburg, Germany)

- **Quantum N-gram Language Models for Tweet Classification**
  Esteban Payares(Universidad Tecnologica de Bolivar, Colombia), Edwin Puertas(Universidad Tecnologica de Bolivar, Colombia) and Juan Carlos Martinez Santos(Northeastern University, United States of America)

CIC Session 2 – Vision/Research: Ransomware, Blockchain and AI

8:30 am – 10:45 am, Room: Breakout 3 - Brookhaven
Session Chair: Qingyang Wang, *Louisiana State University-Baton Rouge, USA*

- **Knowledge Enhanced Deep Learning: Application to Pandemic Prediction**
  John A. Miller(University of Georgia, USA), Nasid Habib Barna(University of Georgia, USA), Subas Rana(University of Georgia, USA), I. Budak Arpinar(University of Georgia, USA) and Ninghao Liu (University of Georgia, USA)

- **Toward Low-Cost and Sustainable IoT Systems for Soil Monitoring in Coastal Wetlands**
  Jianwei Hao(University of Georgia, USA), Rajneesh Sharma(University of Georgia, USA), Mary B. Fleming(University of Georgia, USA), In Kee Kim(University of Georgia, USA), Deepak Mishra(University of Georgia, USA), Sonny Kim(University of Georgia, USA), Lori Sutter and Lakshmish(University of Georgia, USA) Ramaswamy(University of Georgia, USA)

- **Understanding the Behavior of Ransomware: An I/O Request Packet (IRP) Driven Study on Ransomware Detection against Execution Time**
  Md. Ahsan Ayub(Tennessee Technological University, United States of America) and Ambareen Siraj(Tennessee Technological University, United States of America)

- **PRISM: A Blockchain-Enabled Reputation-Based Consensus for Enhancing Scientific Workflow Provenance**
  Matthew Miller(Marshall University, United States of America), Skarlet Williams(Boise State University, United States of America), Gaby G. Dagher(Boise State University, United States of America) and Min Long(Boise State University, United States of America)

- **KNNs of Semantic Encodings for Rating Prediction**
  Léo Laugier(EPFL, Switzerland), Raghuram Vadapalli(Google, United Kingdom), Thomas Bonald(Télécom Paris, Institut Polytechnique de Paris, France) and Lucas Dixon(Google, France)

Coffee Break (15 min)

Keynote 3

11:00 am – 12:00 am, Room: Main Room - Chastain Ballroom
Session Chair: Christen Seifert, *University of Marburg, Germany*

Can Federated Learning be Responsible?

Ling Liu
Georgia Institute of Technology, USA

Lunch Break (90 min)

TPS Session 4 – Vision: AI/LLM Security and Explainability

01:30 pm – 03:45 pm, Room: Main Room - Chastain Ballroom
Session Chair: Li Xiong, Emory University, USA

- **An Investigation on Fragility of Graph Neural Networks: Impact of Node Feature Modification on Graph Classification Accuracy**
  Chengen Wang (University of Texas at Dallas, United States of America), Yan Zhou(University of Texas at Dallas, United States of America), Kankook Jee (University of Texas at Dallas, United States of America) and Murat Kantarcioglu (University of Texas at Dallas, United States of America)

- **Towards Neuro-Symbolic AI for Assured and Trustworthy Human-Autonomy Teaming**
  Danda B. Rawat (Howard University, United States of America)

- **Secure Multimedia Data Systems in the Era of Artificial Intelligence: Significant Progress and Vision for the Future**
  Bhavani Thuraisingham (University of Texas at Dallas, United States of America)

- **Explainable AI for Prioritizing and Deploying Defenses for Cyber-Physical System Resiliency**
  Indrajit Ray(Colorado State University, United States of America), Sarath Sreedharan(Colorado State University, United States of America), Rakesh Podder(Colorado State University, United States of America), Shadaab Kawnain Bashir(Colorado State University, United States of America) and Indrakshi Ray(Colorado State University, United States of America)

- **Invisible Watermarking for Audio Generation Diffusion Models**
  Xirong Cao(Fordham University, United States of America), Xiang Li(Fordham University, United States of America), Divyesh Jadav(IBM Research, United States of America), Yanzhao Wu(Florida International University, United States of America), Zehui Chen(Google, United States of America), Chen Zeng (Google, United States of America) and Wenqi Wei(Fordham University, United States of America)

- **Model Based Risk Assessment and Risk Mitigation Framework for Cyber-Physical Systems**
  Shwetha Gowdanakatte(Colorado State University, United States of America), Indrakshi Ray(Colorado State University, United States of America), Mahmoud Abdelgawad(Colorado State University, United States of America)

TPS Session 5 – Research: Blockchain, Access Control and Privacy

01:30 pm – 03:45 pm, Room: Breakout 1 - Ponce De Leon
Session Chair: Wenbo He, McMaster University, Canada

- **Mind the CORS**
  Matteo Golinelli(University of Trento, Italy), Elham Arshad(University of Trento, Italy), Dmytro Kashchuk (University of Trento, Italy) and Bruno Crispo (University of Trento, Italy)

- **Enabling Collaborative Multi-Domain Applications: A Blockchain-Based Solution with Petri Net Workflow Modeling and Incentivization**
  Reginald Cushing(Netherlands eScience Center, Netherlands), Xin Zhou(University of Amsterdam, Netherlands), Adam Belloum(University of Amsterdam, Netherlands), Paola Grosso(University of Amsterdam, Netherlands), Tom van Engers(University of Amsterdam, Netherlands) and Cees de Laat(University of Amsterdam, Netherlands)

- **Efficiently Supporting Attribute-Based Access Control in Relational Databases**
  Gaurav Meena(Indian Institute of Technology Kharagpur, India), Proteet Paul(Indian Institute of Technology Kharagpur, India) and Shamik Sural(Indian Institute of Technology Kharagpur, India)

- **Toward a (Secure) Path of Least Resistance: An Examination of Usability Challenges in Secure Sandbox Systems**
  Adam Beauchaine(Worcester Polytechnic Institute, United States of America) and Craig Shue(Worcester Polytechnic Institute, United States of America)

- **Ensuring Privacy Policy Compliance of Wearables with IoT Regulations**
  Kelvin Echenim (University of Maryland Baltimore County, United States of America), Lavanya Elluri (Texas A&M University - Central Texas, United States of America) and Karuna Joshi (University of Maryland Baltimore County, United States of America)

- **Balancing Privacy and Accuracy in IoT using Domain-Specific Features for Time Series Classification**
  Pranshul Lakhanpal(California Polytechnic State University, United States of America), Asmita Sharma(California Polytechnic State University, United States of America), Joydeep Mukherjee(California Polytechnic State University, United States of America), Marin Litoiu(York University, Canada) and Sumona Mukhopadhyay(California Polytechnic State University, United States of America)

CogMI Session 3 – Vision: AI, Computer Vision and Applications

01:30 pm – 03:45 pm, Room: Breakout 2 - Roswell
Session Chair: **Paolo Boldi**, *University of Milano, Italy*

- **A Comparative Study of Model-Agnostic and Importance-based Feature Selection Approaches**
  Huanjing Wang (Western Kentucky University, United States of America), Qianxin Liang (Florida Atlantic University, United States of America), John Hancock (Florida Atlantic University, United States of America) and Taghi Khoshgoftaar (Florida Atlantic University, United States of America)

- **Amplifying Object Tracking Performance on Edge Devices**
  Sanjana Vijay Ganesh (Georgia Institute of Technology, United States of America), Yanzhao Wu(Florida International University, United States of America), Gaowen Liu(Cisco Systems, Inc., United States of America), Ramana Kompella(Cisco Systems, Inc., United States of America) and Ling Liu(Georgia Institute of Technology, United States of America)

- **Data Integrity and Artificial Reasoning**
  Adrienne Raglin(Army Research Laboratory, United States of America) and Raha Moraffah(Arizonia State University, United States of America)

- **Statistically-sound Knowledge Discovery from Data: Challenges and Directions**
  Matteo Riondato(Amherst College, United States of America)

- **Comparative Study of Causal Discovery Methods for Cyclic Models with Hidden Confounders**
  Boris Lorbeer(Technical University Berlin, Germany) and Mustafa Mohsen(Technical University Berlin, Germany)

- **Rethinking Learning Rate Tuning in the Era of Large Language Models**
  Hongpeng Jin(Florida International University, United States of America), Wenqi Wei(Fordham University, United States of America), Xuyu Wang(Florida International University, United States of America), Wenbin Zhang(Florida International University, United States of America) and Yanzhao Wu(Florida International University, United States of America)

CIC Session 3 – Vision: LLM, Multi-Modal Learning, Metaverse and Smart Infrastructure

01:30 pm – 03:45 pm, Room: Breakout 3 - Brookhaven
Session Chair: Arun Iyengar*, Cisco Research, USA*

- **Enabling Synergistic Knowledge Sharing and Reasoning in Large Language Models with Collaborative Multi-Agents**
  Ayushman Das(University of Missouri-Kansas City, United States of America), Shu-Ching Chen(University of Missouri-Kansas City, United States of America), Mei-Ling Shyu(University of Missouri-Kansas City, United States of America) and Saad Sadiq(Microsoft, United States of America)

- **Immersive Computing: Vision, Infrastructure, and Use Cases**
  Bo Han(George Mason University, United States of America), Songqing Chen(George Mason University, United States of America), Joel Martin(George Mason University, United States of America), Parth Pathak(George Mason University, United States of America), Amitabh Varshney(University of Maryland, United States of America), Hong Xue(George Mason University,

United States of America), Lap-Fai Yu(George Mason University, United States of America), Jie Zhang(George Mason University, United States of America) and Xiaoquan Zhao(George Mason University, United States of America)

- **Influence Pathway Discovery on Social Media**
  Xinyi Liu(University of Illinois at Urbana-Champaign, United States of America), Ruijie Wang(University of Illinois at Urbana-Champaign, United States of America), Dachun Sun(University of Illinois at Urbana-Champaign, United States of America), Jinning Li(University of Illinois at Urbana-Champaign, United States of America), Christina Youn(University of Illinois at Urbana-Champaign, United States of America), You Lyu(University of Illinois at Urbana-Champaign, United States of America), Jianyuan Zhan(University of Illinois at Urbana-Champaign, United States of America), Dayou Wu(University of Illinois at Urbana-Champaign, United States of America), Xinhe Xu(University of Illinois at Urbana-Champaign, United States of America), Mingjun Liu(University of Illinois at Urbana-Champaign, United States of America), Xinshuo Lei(University of Illinois at Urbana-Champaign, United States of America), Zhihao Xu(University of Illinois at Urbana-Champaign, United States of America), Yutong Zhang(University of Illinois at Urbana-Champaign, United States of America), Zehao Li(University of Illinois at Urbana-Champaign, United States of America), Qikai Yang(University of Illinois at Urbana-Champaign, United States of America) and Tarek Abdelzaher(University of Illinois at Urbana-Champaign, United States of America)

- **A BlackBox Approach to Profile Runtime Execution Dependencies in Microservices**
  Xuhang Gu, Jianshu Liu and Qingyang Wang(Louisiana State University-Baton Rouge, United States of America)

- **Scalable Multimodal Learning and Multimedia Recommendation**
  Jerry Jialie Shen(City, University of London, United Kingdom), Marie Morrison(University of Bristol, United Kindom) and Zhu Li(University of Missouri, United States of America)

Coffee Break (15 min)

Panel 2

04:00pm–06:00pm, Room: Main Room - Chastain Ballroom

AI Impact and Challenges in Industry and Government

Moderator: **James Joshi,** University of Pittsburgh, USA

Panelists (Last Name Alphabetical)

- **Sandeep Gopisetty,** IBM Research - Almaden, USA
- **Arun Iyengar,** Cisco Research, USA
- **Surya Nepal,** CSIRO Data61, Australia
- **Tao Zhang,** NIST, USA

Banquet Dinner (120 min)

IEEE 2023 CIC/CogMI/TPS Joint Conferences

Day 3: Friday, Nov. 3, 2023

CIC/TPS Session 6 – Vision: Security and Trust in LLMs, IoT and Metaverse

8:30 am – 10:45 am, Room: Main Room - Chastain Ballroom
Session Chair: Balaji Palanisamy, *University of Pittsburgh, USA*

- **A Pro-Active Defense Framework for IoT Systems**
  Elisa Bertino(Purdue University, United States of America), Hyunwoo Lee(KENTECH, Republic of Korea), Mengdie Huang(Purdue University, United States of America), Charalampos Katsis(Purdue University, United States of America), Zilin Shen(Purdue University, United States of America), Bruno Ribeiro(Purdue University, United States of America), Daniel de Mello(Purdue University, United States of America) and Ashish Kundu(Cisco Research, United States of America)

- **Beyond Basic Trust: Envisioning the Future of NextGen Networked Systems and Digital Signatures**
  Attila A Yavuz(University of South Florida, United States of America), Kiarash Sedghighadikolaei(University of South Florida, United States of America), Saleh Darzi(University of South Florida, United States of America) and Saif E. Nouma(University of South Florida, United States of America)

- **Digital Twins and the Future of their Use Enabling Shift Left and Shift Right Cybersecurity Operations**
  Ahmad Mohsin(Edith Cowan University Australia, Australia), Helge Janicke(Cyber Security Cooperative Research Centre, Australia), Surya Nepal(Data61, CSIRO, Australia) and David Holmes(Edith Cowan University Australia, Australia)

- **The Dark Side of the Metaverse: Why is it Falling Short of Expectations?**
  Sirisha Talapuru(University of North Texas, United States of America), Ram Dantu(University of North Texas, United States of America), Kritagya Upadhyay(University of North Texas, United States of America), Syed Badruddoja (University of North Texas, United States of America) and Shakila Zaman(University of North Texas, United States of America)

- **Large Language Model-Powered Smart Contract Vulnerability Detection: Vision, Hype and Reality**
  Sihao Hu (Georgia Institute of Technology, United States of America), Tiansheng Huang(Georgia Institute of Technology, United States of America), Fatih İlhan(Georgia Institute of Technology, United States of America), Selim Tekin (Georgia Institute of Technology, United States of America) and Ling Liu(Georgia Institute of Technology, United States of America)

- **Large Language Models and Security**
  Arun Iyengar(Cisco Research, United States of America) and Ashish Kundu (Cisco Research, United States of America)

TPS Session 7 – Research: Security and Privacy

8:30 am – 10:45 am, Room: Breakout 1 - Ponce De Leon
Session Chair: Shamik Sural, Indian Institute of Technology, Kharagpur, India

- **k-Anonymity in Federated Heterogenous Graphs and k-Core Anonymization**
  (Application Paper)
  Mark Dockendorf(University of North Texas, United States of America) and Ram Dantu(University of North Texas, United States of America)

- **Performance Analysis of Homomorphically-Encrypted Heterogeneous Multi-layer Graph Databases**
  (Application Paper)
  John Long(University of North Texas, United States of America), Ram Dantu (University of North Texas, United States of America) and Jacob White(University of North Texas, United States of America)

- **Harvesting Security: A Semantically Enriched Access Control Architecture for Smart Farms**
  (Application Paper)
  Ghadeer Yassin(University of Georgia, United States of America) and Lakshmish Ramaswamy(University of Georgia, United States of America)

- **Peculiarity and diversity measures to evaluate attribute-based access rules**
  (Application Paper)
  Abner Perez-Haro(Abner Perez-Haro, Mexico) and Arturo Diaz-Perez(Abner Perez-Haro, Mexico)

- **Quantitative Risk Analysis With Qualitative Statements**
  (Application Paper)
  Karim Elhammady(University of Waterloo, Canada) and Sebastian Fischmeister(University of Waterloo, Canada)

CogMI Session 4 – Research / Vision: AI and Machine Learning

8:30 am – 10:45 am, Room: Breakout 2 - Roswell
Session Chair: Indrakshi Ray, *Colorado State University, USA*

- **The Intersection of Usability Evaluation and Machine Learning in Software Systems**
  Richard Torres Molina(Virginia Tech, United States of America) and Mohammed Seyam(Virginia Tech, United States of America)

- **Prompt-to-OS (P2OS): Revolutionizing Operating Systems and Human-Computer Interaction with Integrated AI Generative Models**
  Gabriele Tolomei(Sapienza University of Rome, Italy), Cesare Campagnano(Sapienza University of Rome, Italy), Fabrizio Silvestri(Sapienza University of Rome, Italy) and Giovanni Trappolini(Sapienza University of Rome, Italy)

- **ABC: Automatic Bottom-up Construction of Configuration Knowledge Base for Multi-Vendor Networks**
  Wenlong Ding(The Chinese University of Hong Kong , Hong Kong, China), Libin Liu(Zhongguancun Laboratory, China), Li Chen(Zhongguancun Laboratory, China) and Hong Xu(The Chinese University of Hong Kong , Hong Kong, China)

- **CommunityAI: Towards Community-based Federated Learning**

Ilir Murturi(Vienna University of Technology, Austria), Praveen Kumar Donta(Vienna University of Technology, Austria) and Schahram Dustdar(Vienna University of Technology, Austria)

- **Link Streams as a Generalization of Graphs and Time Series**
  Matthieu Latapy(Sorbonne Université, France) and Bautista Esteban(IMT Atlantique, France)

- **Revisiting Metric Space Similarity Methods For High Performance Deep Embedding Learning**
  Chungheon Yi(Inha University, South Korea), Wonik Choi(Inha University, South Korea) and Ling Liu(Georgia Institute of Technology, United States of America)

CogMI Session 5 – Research: AI and Applications

8:30 am – 10:45 am, Room: Breakout 3 - Brookhaven
Session Chair: Yanzhao Wu, *Florida International University, USA*

- **Evaluate Effectiveness of NAO Robot to Train Children with Autism Spectrum Disorder (ASD)**
  Masud Karim(University of Dhaka, Bangladesh), Md. Solaiman Mia((Green University of Bangladesh, Bangladesh)), Saifuddin Md. Tareeq(University of Dhaka, Bangladesh) and Md Hasanuzzaman(Southern Arkansas University, United States of America)

- **Improving Time-series Classification Accuracy based on Temporal Feature Representation Learning using CRU-LSTM Autoencoder**
  Dohee Kim(Pusan National University, South Korea), Sunghyun Sim(Pusan National University, South Korea), Bori Yoon(Pusan National University, South Korea), Ling Liu(Georgia Institute of Technology , United States of America) and Hyerim Bae(Pusan National University, South Korea)

- **Cognitive Inspired Automatic Chunking and Forgetting for Multimodal Task in Robots**
  Shweta Singh(IIIT, Hyderabad, India), Vedant Ghatnekar(MIT WPU, Pune, India) and Sudaman Katti(VIT, Pune, India)

- **Enhancing Solar Flare Prediction with Innovative Data-Driven Labels**
  (Application Paper)
  Jinsu Hong(Georgia State University, United States of America), Anli Ji(Georgia State University, United States of America), Chetraj Pandey(Georgia State University, United States of America) and Berkay Aydin(Georgia State University, United States of America)

- **Active Region-based Flare Forecasting with Sliding Window Multivariate Time Series Forest Classifiers**
  (Application Paper)
  Anli Ji(Georgia State University, United States of America) and Berkay Aydin(Georgia State University, United States of America)

- **Skills Extraction from Entities in Arabic CVs**
  (Application Paper)
  Mohamed Abdul Karim Sadiq(University of Technology and Applied Sciences, Oman), Shanmugam Thirumurugan(University of Technology and Applied Sciences, Oman), Nasser Alfannah(Ministry of Transport, Communications and Information Technology, Oman) and Firdous Kausar(Fisk University, United States of America)

Industry Session

8:30 am – 10:45 am, Room: Breakout 4 - Peachtree
Session Chair: Indrajit Ray, *Colorado State University, USA*

- **A Comprehensive Analysis of Trust, Privacy, and Security Measures in the Digital Age**
  Debashis Das(University of Kalyani, Kalyani, India), Sourav Banerjee(Kalyani Government Engineering College, India), Pushpita Chatterjee(Howard University, United States of America) and Uttam Ghosh(Meharry Medical College, United States of America)

- **Forecasting the Spread of Toxicity on Twitter**
  Aatman Vaidya(Ahmedabad University, India), Seema Nagar(IBM Research India) and Amit A. Nanavati(Ahmedabad University, India)

- **Secured Data Movement using Data Ring Fencing**
  Aditya Nangia(IIITD, India), Saksham Bhupal(IIITD, India), Mukesh Mohania(IIITD, India) and Chinmay Kundu(KIIT, India)

- **The Effect of Human v/s Synthetic Test Data and Round-tripping on Assessment of Sentiment Analysis Systems for Bias**
  Kausik Lakkaraju(University of South Carolina, United States of America), Aniket Gupta(Netaji Subhas University of Technology, India), Biplav Srivastava(University of South Carolina, United States of America), Marco Valtorta(University of South Carolina, United States of America) and Dezhi Wu(University of South Carolina, United States of America)

- **CRISP: Change Risk for IT Service Providers**
  Arun Ayachitula(Kyndryl, United States of America) and Upendra Sharma(Kyndryl, United States of America)

- **SOC and Academia – Building Resilient Systems**
  Abhilasha Bhargav-Spantzel (Microsoft, United States of America) and Carson Zimmerman (Microsoft, United States of America)

- **Bridging the Gap: Industry Perspectives and Trends in Cloud Security, and Opportunities for Collaborative Research**
  Sarabjeet Chugh (Cisco Systems, Inc., United States of America)

Coffee Break (15 min)

Keynote 4

11:00 am-12:00 am, Room: Main Room - Chastain Ballroom
Session Chair: James Joshi, *University of Pittsburgh, USA*

Advancing Technology, Innovation and Partnerships

Erwin Gianchandani
National Science Foundation (NSF), USA

Lunch Break (90 min)

Panel 3

01:30pm–03:30pm, Room: Main Room - Chastain Ballroom

Grand Challenges in Cyber Security and Privacy

Moderator: **James Joshi,** University of Pittsburgh, USA

Panelists (Last Name Alphabetical)

- **Elisa Bertino,** Purdue University, USA
- **Anupam Joshi,** University of Maryland Baltimore County, USA
- **Vladimir, Kolesnikov,** Georgia Institute of Technology
- **Elaine Shi,** Carnegie Mellon University, USA

Coffee Break (60 min)

Closing Remarks (60 min)

WAAM 2023 Program

Time	Event/Panel
08:00am-08:30am	Breakfast
08:30am-09:15am	Panel 1: Identifying and Measuring Properties of Autonomous/AI/ML Systems • Junhua Ding, University of North Texas • Erin Lanus, Virginia Tech • Adam Porter, University of Maryland • Sandeep Neema, Vanderbilt University • David Stracuzzi, Sandia National Laboratories
09:15am-10:45am	Panel 2: Identifying Risk and Mitigation Strategies for Autonomous/AI/ML Systems • Darren Cofer, Collins Aerospace • Cody Fleming, Iowa State • Junhua Ding, University of North Texas • Ering Lanus, Virginia Tech • Carl Elks, Virginia Commonwealth University
10:45am-11:00am	Break
11:00am-12:00pm	Panel 3: Designing Autonomous/AI/ML Systems for Assurance • Cody Fleming, Iowa State • Stephen Magill, Sonatype • Alessandro Pinto, JPL- NASA Ames • Jaganmohan Chadrasekaran, Virginia Tech • Sandeep Neema, Vanderbilt University
12:00pm-01:30pm	Lunch (provided)
01:30pm-02:30pm	Panel 4: The impact of AI/ML in Application Security • Alwyn Goodloe, NASA Langley Junhua Ding, University of North Texas • Stephen Magill, Sonatype • Joanna DeFranco, Penn State
02:30pm-03:45pm	Panel 5: Societal Implications: Awareness, Education, Training and Certification • Darren Cofer, Collins Aerospace • Alwyn Goodloe, NASA Langley • Cate Richards, Sonatype • Phil Laplante, US National Institute of Standards and Technologies
03:45pm-04:00pm	Break
04:00pm-06:00pm	Panel 6: Industry-Government perspective (joint with TSP Conference) TBA
06:00pm-8:00pm	Dinner

dDEI Workshop

Session Chairs: Kimberley Hemmings-Jarrett, Penn State University – Abington

Presenters

Swathi Jagannath, PhD
User Experience Researcher II, Microsoft

Houda El Mimouni, PhD
Computing Innovation (CI) Fellow, Indiana University Bloomington

Ricardo Anderson, PhD
Lecturer, Department of Computing, The University of the West Indies, Mona

Anietie Andy, PhD
Assistant Professor, Electrical Engineering and Computer Science, Howard University

Glenville Mcleod, PhD Candidate
Assistant Lecturer, The University of the West Indies, Mona