

# 2025 IEEE 7th International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications (TPS-ISA)

## TPS-ISA 2025

### Table of Contents

Message from the TPS-ISA 2025 Chairs .....	xv
Organizing Committee .....	xvii
Steering Committee .....	xviii
Technical Program Committee .....	xix
Keynotes .....	xx
Plenary Panel .....	xxii

### TPS Research Session

Enabling Privacy-Preserving Model Evaluation in Federated Learning via Fully Homomorphic Encryption .....	1
<i>Cem Ata Baykara (University of Tübingen, Germany), Ali Burak Ünal (University of Tübingen, Germany), and Mete Akgün (University of Tübingen, Germany)</i>	
HERL: Tiered Federated Learning with Adaptive Homomorphic Encryption Using Reinforcement Learning .....	11
<i>Jiaxang Tang (University of Minnesota, USA), Zeshan Fayyaz (University of Waterloo, Canada), Mohammad A. Salahuddin (University of Waterloo, Canada), Raouf Boutaba (University of Waterloo, Canada), Zhi-Li Zhang (University of Minnesota, USA), and Ali Anwar (University of Minnesota, USA)</i>	
PPFL-RDSN: Privacy-Preserving Federated Learning-Based Residual Dense Spatial Networks for Encrypted Lossy Image Reconstruction .....	21
<i>Peilin He (University of Pittsburgh, USA) and James Joshi (University of Pittsburgh, USA)</i>	
One-Shot Secure Aggregation: A Hybrid Cryptographic Protocol for Private Federated Learning in IoT .....	32
<i>Imraul Kayes Emmaka (University of Arkansas at Little Rock, USA) and Tran Viet Xuan Phuong (University of Arkansas at Little Rock, USA)</i>	

RBBB: A Representation-Based Framework for Edge-Case Backdoor Defense in Federated Learning .....	43
<i>Samir Poudel (Middle Tennessee State University, TN), Kritagya Upadhyay (Middle Tennessee State University, TN), and Jiblal Upadhya (Lander University, S.C.)</i>	
Enhancing Resilience in Industrial Control Systems: Rapid Attack Detection, Recovery, and Monotonicity Preservation Through STL-GT Online Monitoring .....	54
<i>Chidi Agbo (University of Nebraska at Kearney, USA) and Hoda Mehrpouyan (Boise State University, USA)</i>	
Robust Physically Realizable Backdoor Attack .....	66
<i>Md Jahirul Islam (Kennesaw State University, USA) and Kazi Aminul Islam (Kennesaw State University, USA)</i>	
Fidelity-Optimizing Defense Mechanism Against Membership Inference Attacks .....	76
<i>Md Faisal Ahmed (George Mason University) and Zhengdao Wang (George Mason University)</i>	
NatGVD: Natural Adversarial Example Attack Towards Graph-Based Vulnerability Detection .....	89
<i>Avilash Rath (The University of Texas at Dallas), Weiliang Qi (The University of Texas at Dallas), Youpeng Li (The University of Texas at Dallas), and Xinda Wang (The University of Texas at Dallas)</i>	
Explainable but Vulnerable: Adversarial Attacks on XAI Explanation in Cybersecurity Applications .....	101
<i>Maraz Mia (Tennessee Tech University, USA) and Mir Mehedi Ahsan Pritom (Tennessee Tech University, USA)</i>	
Anomaly Detection in Graphs via Topology-Aware Attention Mechanisms .....	111
<i>Narges Alipourjehdi (Toronto Metropolitan University, Canada) and Ali Miri (Toronto Metropolitan University, Canada)</i>	
It's About Time!: Exploiting Timing Variance for IoT Device-Type Fingerprinting .....	119
<i>Maxwel Bar-on (Colorado State University, USA), Alanood Alqobaisi (Colorado State University, USA), Bruhadeshwar Bezawada (Southern Arkansas University, USA), Indrakshi Ray (Colorado State University, USA), and Indrajit Ray (Colorado State University, USA)</i>	
Data Access Control in Large Language Models .....	130
<i>Nouha Oualha (Université Paris-Saclay, France) and Christophe Janneteau (Université Paris-Saclay, France)</i>	
Clone What You Can't Steal: Black-Box LLM Replication via Logit Leakage and Distillation .....	140
<i>Kanchon Gharami (Embry-Riddle Aeronautical University, USA), Hansaka Aluvihare (Embry-Riddle Aeronautical University, USA), Shafika Showkat Moni (Embry-Riddle Aeronautical University, USA), and Berker Peköz (Embry-Riddle Aeronautical University, USA)</i>	
PRvL: Quantifying the Capabilities and Risks of Large Language Models for PII Redaction .....	148
<i>Leon Garza (The University of Texas at El Paso, USA), Anantaa Kotal (The University of Texas at El Paso, USA), Aritran Piplai (The University of Texas at El Paso, USA), Lavanya Elluri (Texas A&amp;M University-Central Texas, USA), Prajit Kumar Das (Cisco Systems Inc, USA), and Aman Chadha (Amazon Web Services, USA)</i>	

LLMalMorph: On The Feasibility of Generating Variant Malware Using Large-Language-Models ..	160
<i>Md Ajwad Akil (Purdue University, USA), Adrian Shuai Li (Purdue University, USA), Imtiaz Karim (The University of Texas at Dallas, USA), Arun Iyengar (Intelligent Data Management and Analytics, LLC, USA), Ashish Kundu (Cisco Research, USA), Vinny Parla (Cisco Systems, Inc, USA), and Elisa Bertino (Purdue University, USA)</i>	
CipherBERT: A Systematic Framework for High-Accuracy Encrypted Transformer Inference .....	172
<i>Nisarg Bhaosar (Indian Institute of Technology Kharagpur, India) and Zaid Ahmed Khan (Indian Institute of Technology Kharagpur, India)</i>	
CoDICE: Roll the DICE for Firmware Attestation .....	183
<i>Rakesh Podder (Colorado State University, USA), Jason Simental (Colorado State University, USA), Elmaddin Azizli (Colorado State University, USA), Bharadwaj Mantha (Colorado State University, USA), and Indrajit Ray (Colorado State University, USA)</i>	
Limitations of Watermarking AI-Generated Speech Using AudioSeal .....	197
<i>Shameer Faziludeen (University College Cork, Ireland), Arun Sankar M. S. (South East Technological University, Ireland), Phillip L. De Leon (University of Colorado Denver, USA), and Utz Roedig (University College Cork, Ireland)</i>	
Diffusion Based Face Generation via Image Editing and Image Morphing .....	207
<i>Liyue Fan (University of North Carolina at Charlotte, USA) and Joseph Roberson (University of North Carolina at Charlotte, USA)</i>	
EDL: Efficient Data-Oblivious Loops .....	213
<i>Biniyam Tiruye (University of Michigan, USA), Lauren Biernacki (Lafayette College, USA), and Todd Austin (University of Michigan, USA)</i>	
Decoding the Decoders: An Empirical Study of Reverse Engineering Questions on Stack Exchange .....	226
<i>Md Rakibul Islam (Lamar University, USA), Md Humaun Kabir (Lamar University, USA), and Anwarul Islam Sifat (Lamar University, USA)</i>	
PQC-LEO: An Evaluation Framework for Post-Quantum Cryptographic Algorithms .....	237
<i>Callum Turino (Edinburgh Napier University, UK), William J. Buchanan (Edinburgh Napier University, UK), Owen Lo (Edinburgh Napier University, UK), and Christoph Thümmel (6GHI, Germany)</i>	
Explainable AI in Data Poisoning Threat Models Across the CIA Triad: A Smart Grid Case Study .....	248
<i>Gustavo Sánchez (Karlsruhe Institute of Technology (KIT), Germany), Ghada Elbez (Karlsruhe Institute of Technology (KIT), Germany), and Veit Hagenmeyer (Karlsruhe Institute of Technology (KIT), Germany)</i>	

## TPS Application Session

A Privacy-Fidelity Tradeoff Framework in Post-Processed Machine Learning .....	259
<i>Md Faisal Ahmed (George Mason University) and Zhengdao Wang (George Mason University)</i>	

Learning from Literature: A Retraining-Free Framework for LLM Jailbreak Defense via NLP-Based Adversarial Literature Analysis .....	270
<i>Sheikh Samit Muhaimin (University of Notre Dame, USA) and Spyridon Mastorakis (University of Notre Dame, USA)</i>	
Images in Motion?: A First Look into Video Leakage in Collaborative Deep Learning .....	282
<i>Md Fazle Rasul (Colorado State University, USA), Alanood Alqobaisi (Colorado State University, USA), Bruhadeshwar Bezawada (Southern Arkansas University, USA), and Indrakshi Ray (Colorado State University, USA)</i>	
Privacy-Preserving AI-Enabled Decentralized Learning and Employment Records System .....	293
<i>Yuqiao Xu (Case Western Reserve University, USA), Mina Namazi (Case Western Reserve University, USA), Sahith Reddy Jalapally (Case Western Reserve University, USA), Osama Zafar (Case Western Reserve University, USA), Youngjin Yoo (The London School of Economics and Political Science, United Kingdom), and Erman Ayday (Case Western Reserve University, USA)</i>	
FALCON: Federated Anomaly Learning and COLlaborative Network for Secure Autonomous Vehicles .....	304
<i>Riadh Ben Chaabene (École de technologie supérieure (ÉTS), Canada), Darine Amayed (École de technologie supérieure (ÉTS), Canada), Fehmi Jaafar (Université du Québec à Chicoutimi (UQAC), Canada), and Mohamed Cheriet (École de technologie supérieure (ÉTS), Canada)</i>	
MAVUL: Multi-Agent Vulnerability Detection via Contextual Reasoning and Interactive Refinement .....	314
<i>Youpeng Li (University of Texas at Dallas, USA), Kartik Joshi (University of Texas at Dallas, USA), Xinda Wang (University of Texas at Dallas, USA), and Eric Wong (University of Texas at Dallas, USA)</i>	
Leveraging Transformer Models and eXplainable Reinforcement Learning Methods for Advanced Intrusion Detection and Response System .....	325
<i>Mohammad Ghasemigol (Old Dominion University, USA) and Daniel Takabi (Old Dominion University, USA)</i>	
GPS Spoofing Attacks and Pilot Responses Using a Flight Simulator Environment .....	334
<i>Mathilde Durieux (Ecole de l'air et de l'espace Chemin St Jean, France), Kayla D. Taylor (Embry-Riddle Aeronautical University, USA), Laxima Niure Kandel (Embry-Riddle Aeronautical University, USA), and Deepti Gupta (Texas A&amp;M University-Central Texas, TX)</i>	
VulnDetective: Using LLM Agents to Analyze Common Weaknesses and Identify Smart Contract Vulnerabilities .....	342
<i>Thanmai Mandala (University of Texas at Dallas ), Cora Zeger (University of Denver), Tessa E. Andersen (Brigham Young University), Gaby G. Dagher (Boise State University ), and Jun Zhuang (Boise State University )</i>	
XAST: Explainable AST-Transformer for Smart Contract Vulnerability Detection .....	352
<i>Harshith Sai Veeraiah (California State University, Sacramento), Syed Badruddoja (California State University, Sacramento), and Ram Dantu (University of North Texas)</i>	

Guiding Reinforcement Learning Using Uncertainty-Aware Large Language Models .....	363
<i>Maryam Shoaebinaeini (University of Kentucky) and Brent Harrison (University of Kentucky)</i>	

## TPS Invited Session

Security of Operations on Random Numbers .....	372
<i>Tejas Sharma (IIT Bombay, India) and Ashish Kundu (Cisco Research, USA)</i>	
Experiences Building Enterprise-Level Privacy-Preserving Federated Learning to Power AI for Science .....	382
<i>Zilinghan Li (Argonne National Laboratory; National Center for Supercomputing Applications), Aditya Sinha (Argonne National Laboratory; National Center for Supercomputing Applications; University of Illinois at Urbana-Champaign), Yijiang Li (Argonne National Laboratory), Kyle Chard (Argonne National Laboratory; The University of Chicago), Kibaek Kim (Argonne National Laboratory; The University of Chicago), and Ravi Madduri (Argonne National Laboratory; The University of Chicago)</i>	
Detection of Blacktopped Counterfeit ICs Using Surface Texture Analysis .....	392
<i>John M. Klamut (University of Pittsburgh, USA), Mai Abdelhakim (University of Pittsburgh, USA), Samuel J. Dickerson (University of Pittsburgh, USA), Ashish Avachat (University of Pittsburgh, USA), Heng Ban (University of Pittsburgh, USA), and Philip Santillo (University of Pittsburgh, USA)</i>	
Upgrade or Switch: Do We Need a Next-Gen Trusted Architecture for the Internet of AI Agents? .....	399
<i>Ramesh Raskar (Massachusetts Institute of Technology), Pradyumna Chari (Massachusetts Institute of Technology), Mahesh Lambe (Independent Researcher), Robert Lincourt (Dell Technologies), Raghu Bala (Synergetics AI), Aditi Joshi (Independent Researcher), Jared Grogan (Independent Researcher), Abhishek Singh (Massachusetts Institute of Technology), Ayush Chopra (Massachusetts Institute of Technology), Rajesh Ranjan (Independent Researcher), Shailja Gupta (Independent Researcher), Dimitris Strepalis (Flower AI), Maria Gorskikh (Independent Researcher), and Sichao Wang (Cisco Systems)</i>	
Challenges in Identifying Illicit Actors in Financial Networks .....	409
<i>Amro Aljundi (University of Virginia, USA), Abhijin Adiga (University of Virginia, USA), Philip Potter (University of Virginia, USA), Samarth Swarup (University of Virginia, USA), Anil Vullikanti (University of Virginia, USA), and Madhav Marathe (University of Virginia, USA)</i>	

# IEEE Workshop on Security and Resiliency of Critical Infrastructure and Space Technologies (IEEE SR-CIST 2025)

A Multi-Layered Embedded Intrusion Detection Framework for Programmable Logic Controllers .	419
<i>Rishabh Das (Ohio University, USA), Aaron Werth (The University of Alabama in Huntsville, USA), and Tommy Morris (The University of Alabama in Huntsville, USA)</i>	
Investigating Physical Consequences of Cyber-Attacks Using a Cyber-Physical Model of a Compressor Station .....	427
<i>Andrew S. Hahn (Sandia National Laboratories, NM), Adam J. Beauchaine (Sandia National Laboratories, NM), Lee T. Maccarone (Sandia National Laboratories, NM), Titus A. Gray (Sandia National Laboratories, NM), and Robert S. Lois (Sandia National Laboratories, NM)</i>	
TPM-Based Continuous Remote Attestation and Integrity Verification for 5G VNFs on Kubernetes .....	435
<i>Al Nahian Bin Emran (George Mason University, USA), Rajendra Upadhyay (George Mason University, USA), Rajendra Paudyal (George Mason University, USA), Lisa Donnan (George Mason University, USA), and Duminda Wijesekera (George Mason University, USA)</i>	
Resilience to Dynamic Load Attacks Under AI Demand and Hyperscale Data Centers .....	445
<i>Masoud Barati (University of Pittsburgh, USA)</i>	
Quantitative Analysis of UAV Intrusion Mitigation for Border Security in 5G with LEO Backhaul Impairments .....	455
<i>Rajendra Upadhyay (George Mason University, USA), Al Nahian Bin Emran (George Mason University, USA), Rajendra Paudyal (George Mason University, USA), Lisa Donnan (George Mason University, USA), and Duminda Wijesekera (George Mason University, USA)</i>	
Route Choice Prediction Through User Behavior Analysis: Towards Robustness Assessment Under External Perturbations .....	464
<i>Gustavo Sánchez (Karlsruhe Institute of Technology, Germany), Fatih Ünal (Karlsruhe Institute of Technology, Germany), and Alexandra Wins (Mercedes-Benz Tech Innovation GmbH, Germany)</i>	
Grid-Computer Symbiosis: Towards the Industrial Internet of Things .....	469
<i>Danielle McGuire (Duquesne Light Company, PA)</i>	
Space-Based Fog Computing Across LEO and MEO Constellations for On-Orbit Hypersonic Detection and Space Domain Awareness .....	479
<i>Jackson Artis (Cornell University, USA) and Gregory Falco (Cornell University, USA)</i>	
WaveVerif: Acoustic Side-Channel Based Verification of Robotic Workflows .....	489
<i>Zeynep Yasemin Erdogan (Newcastle University), Shishir Nagaraja (Newcastle University), Chuadhry Mujeeb Ahmed (Newcastle University), and Ryan Shah (Sapphire)</i>	

# The 1st IEEE Workshop on Healthcare and Medical Device Security, Privacy, Resilience, and Trust (IEEE HMD-SPiRiT 2025)

AegisBlock: A Privacy-Preserving Medical Research Framework Using Blockchain .....	500
<i>Calkin Garg (Georgia Institute of Technology), Omar Rios Cruz (California State University, Stanislaus), Tessa E. Andersen (Brigham Young University), Gaby G. Dagher (Boise State University), Donald Winiacki (Boise State University), and Min Long (Boise State University)</i>	
Exploring Membership Inference Vulnerabilities in Clinical Large Language Models .....	509
<i>Alexander Nemecek (Case Western Reserve University, USA), Zebin Yun (Tel Aviv University, Israel), Zahra Rahmani (Case Western Reserve University, USA), Yaniv Harel (Tel Aviv University, Israel), Vipin Chaudhary (Case Western Reserve University, USA), Mahmood Sharif (Tel Aviv University, Israel), and Erman Ayday (Case Western Reserve University, USA)</i>	
Convergence of Operational Technology/Industrial Control Systems/Internet of Medical Things: Internet-Exposed Medical Device Threats .....	517
<i>J. Malakai Bailey (Alyn, Inc., USA), William Yurcik (Centers for Medicare &amp; Medicaid Services (CMS), USA), O. Sami Saydjari (Dartmouth College, USA), Rodolfo da Silva Avelino (Insper, Brazil), João Luisi Vieira (Insper, Brazil), Pedro Umbelino (Bitsight Technologies, USA), and Gregory Pluta (University of Illinois at Urbana-Champaign, USA)</i>	
Examining The CoVCues Dataset: Supporting COVID Infodemic Research Through A Novel User Assessment Study .....	526
<i>Shreetika Poudel (Northern Kentucky University, USA) and Ankur Chattopadhyay (Northern Kentucky University, USA )</i>	
Evaluating Security Features in Mobile Health Apps: A Systematic Review .....	536
<i>Yuanyuan Cao (University of Pittsburgh, USA), Yi Xu (University of Pittsburgh, USA), and Leming Zhou (University of Pittsburgh, USA)</i>	
A High-Assurance Systems Approach to Medical Device Security .....	543
<i>Daniel G Cole (University of Pittsburgh, PA) and William W Clark (University of Pittsburgh, PA)</i>	
An Unsupervised Domain Adaptation Method to Enhance Diagnostic Model Resilience on Heterogeneous Medical Imaging Data .....	545
<i>Zhiwei Gong (University of Pittsburgh, USA), Dooman Arefan (University of Pittsburgh, USA), Wendie A. Berg (University of Pittsburgh, USA), and Shandong Wu (University of Pittsburgh, USA)</i>	
Privacy at Scale in Networked Healthcare .....	551
<i>M. Amin Rahimian (University of Pittsburgh), Benjamin Panny (University of Pittsburgh), and James B.D. Joshi (University of Pittsburgh)</i>	

# The Second IEEE Workshop on Quantum Intelligence, Learning and Security (QuILLS 2025)

Architectural Approaches to Fault-Tolerant Distributed Quantum Computing and Their Entanglement Overheads .....	561
<i>Nitish Chandra (University of Pittsburgh, USA), Eneet Kaur (Cisco Quantum Lab, USA), and Kaushik Seshadreesan (University of Pittsburgh, USA)</i>	
Not All Qubits are Utilized Equally .....	573
<i>Jeremie Pope (Pennsylvania State University, USA) and Swaroop Ghosh (Pennsylvania State University, USA)</i>	
Quantum Heuristics for Linear Optimization over Large Separable Operators .....	580
<i>Ankith Mohan (Virginia Tech, USA), Tobias Haug (Technology Innovation Institute, UAE), Kishor Bharti (Agency for Science, Technology and Research, Singapore), and Jamie Sikora (Virginia Tech, USA)</i>	
Towards Quantum-Driven Multimodal Machine Learning: Methods, Challenges, and Future Directions .....	590
<i>Debashis Das (Department of Computer Science and Data Science, Meharry Medical College, USA), Jaclyn Claiborne (Department of Computer Science and Data Science, Meharry Medical College, USA), Lexus Brinkley-Tapp (Department of Computer Science and Data Science, Meharry Medical College, USA), Mikel Houston (Department of Computer Science and Data Science, Meharry Medical College, USA), Pushpita Chatterjee (Department of Computer Science and Data Science, Meharry Medical College, USA), and Uttam Ghosh (Department of Computer Science and Data Science, Meharry Medical College, USA)</i>	
Quantum-Resistant Networks Using Post-Quantum Cryptography .....	600
<i>Xin Jin (University of Pittsburgh, USA), Nitish Kumar Chandra (University of Pittsburgh, USA), Mohadeseh Azari (University of Pittsburgh, USA), Kaushik P. Seshadreesan (University of Pittsburgh, USA), and Junyu Liu (University of Pittsburgh, USA)</i>	
Towards Symmetry-Aware Efficient Simulation of Quantum Systems and Beyond .....	606
<i>Min Chen (University of Pittsburgh, USA), Minzhao Liu (University of Chicago, USA; Argonne National Laboratory, USA), Changhun Oh (Korea Advanced Institute of Science and Technology, Korea; University of Chicago; USA), Liang Jiang (University of Chicago, USA), Yuri Alexeev (Argonne National Laboratory, USA; NVIDIA Corporation, USA), and Junyu Liu (University of Pittsburgh, USA; University of Chicago, USA)</i>	
A Decentralized Framework for Auditing Large Language Model Reasoning .....	610
<i>Morris Yu-Chao Huang (University of North Carolina at Chapel Hill, USA), Zhen Tan (Arizona State University, USA), Mohan Zhang (University of North Carolina at Chapel Hill, USA), Pingzhi Li (University of North Carolina at Chapel Hill, USA), Zezhen Ding (The Hong Kong University of Science and Technology, China), Zhuo Zhang (Columbia University, USA), and Tianlong Chen (University of North Carolina at Chapel Hill, USA)</i>	
Perspective on AI-Empowered Design of Realistic Quantum Optical Device .....	613
<i>Chaohan Cui (University of Maryland, USA), Kailu Zhou (University of Michigan, USA), and Zheshen Zhang (University of Michigan, USA)</i>	

## IEEE Workshop on Distributed, Secure, and Trustworthy Intelligence with LLMs (IEEE DISTILL 2025)

Measuring Privacy Literacy on Generative AI: A Pilot Study of Generation Z .....	616
<i>Jing Hua (La Roche University, USA) and Wenli Wang (Robert Morris University, USA)</i>	
Detecting and Correcting Hallucinations in Paragraph-Level Text with Ensemble-Based Evaluation .....	623
<i>Shivangi Tripathi (Texas State University, USA) and Heena Rathore (Texas State University, USA)</i>	
Trustworthy LLM-Mediated Communication: Evaluating Information Fidelity in LLM as a Communicator (LAAC) Framework in Multiple Application Domains .....	632
<i>Mohammed Musthafa Rafi (Iowa State University, USA), Adarsh Krishnamurthy (Iowa State University, USA), and Aditya Balu (Iowa State University, USA)</i>	
Topic Modeling Analysis of Ethical Framework Separability in LLM-Generated Moral Justifications .....	640
<i>Bishal Thapa (Texas State University, TX) and Heena Rathore (Texas State University, TX)</i>	
The Mediating Role of Explainable AI on Phishing Susceptibility .....	650
<i>Masialeti Masialeti (Robert Morris University, USA) and Wenli Wang (Robert Morris University, USA)</i>	
Machine Learning-Based Frameworks for Malware Detection with SHAP Explainability .....	655
<i>Afia Darko Asante (The University of Akron, USA), Sumaila Iddrisu (The University of Akron, USA), and Nadhem Ebrahim (The University of Akron, USA)</i>	

## IEEE Workshop on Trustworthy and Privacy-Preserving Human-AI Collaboration (IEEE TPHAC 2025)

RegEase: Simplifying Insurance Compliance .....	665
<i>Samhitha Poreddy (Verisk Analytics)</i>	
Backdoor-Aware Adaptive Aggregation for Wireless Ad Hoc Federated Learning .....	670
<i>Atsuya Muramatsu (The University of Tokyo, Japan) and Hideya Ochiai (The University of Tokyo, Japan)</i>	
Certified Attribute Privacy in GAN Latent Space .....	678
<i>Jamil Arbas (Toronto Metropolitan University, Canada), Shadan Ghaffaripour (Toronto Metropolitan University, Canada), and Ali Miri (Toronto Metropolitan University, Canada)</i>	
Voice Design and Trust in Automated Vehicles: Findings and a Research Agenda .....	688
<i>Jiongyu Chen (Arizona State University, USA) and Qiaoning Zhang (Arizona State University, USA)</i>	
The Role of Perceived Social Identity in Human-AI Collaboration .....	697
<i>Jessica K. Barfield (University of Kentucky, USA)</i>	

Quantifying Trust in Human-AI Teams: A Statistical Framework for Task-Based Calibration of AI Autonomy in Compliance Auditing .....	703
<i>Priya Mohan (Independent Researcher, USA), Yugandhar Reddy Suthari (University of the Cumberlands, USA), and Sahil Dhir (Independent Researcher, USA)</i>	
Uncertainty Quantification for Deep Learning-Based Medical Imaging Classification Model Evaluation and Individualized Risk Estimation .....	717
<i>Jiren Li (University of Pittsburgh, USA), Dooman Arefan (University of Pittsburgh, USA), and Shandong Wu (University of Pittsburgh, USA)</i>	
Multimodal Deep Fusion Architecture for Human Activity and Fall Detection in Elderly Care .....	724
<i>Debashis Das (Meharry Medical College, Nashville, TN, USA), Laure Bien Aime (Meharry Medical College, Nashville, TN, USA), Pushpita Chatterjee (Meharry Medical College, Nashville, TN, USA), and Uttam Ghosh (Meharry Medical College, Nashville, TN, USA)</i>	
<b>Author Index .....</b>	<b>733</b>