2023 5th IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA 2023)

Atlanta, Georgia, USA
1 – 3 November 2023

IEEE

IEEE Catalog Number: CFP23V08-POD
ISBN: 979-8-3503-2386-3

****** This is a print representation of what appears in the IEEE Digital Library. Some format issues inherent in the e-media version may also appear in this print version.***

IEEE Catalog Number: CFP23V08-POD
ISBN (Print-On-Demand): 979-8-3503-2386-3
ISBN (Online): 979-8-3503-2385-6

Additional Copies of This Publication Are Available From:

Curran Associates, Inc
57 Morehouse Lane
Red Hook, NY 12571 USA
Phone: (845) 758-0400
Fax: (845) 758-2633
E-mail: curran@proceedings.com
Web: www.proceedings.com

2023 5th IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA)

TPS-ISA 2023

Table of Contents

Message from the General Chairs and PC Chairs ..... **xi**
Organizing Committee ..... **xii**
Technical Program Committee ..... **xiii**
Steering Committee ..... **xiv**
Keynote ..... **xv**
Plenary Panel ..... **xvi**

Vision: Trust and Privacy I

Ensuring Trust in Genomics Research 1
Erman Ayday (Case Western Reserve University, USA), Jaideep Vaidya (Rutgers University, USA), Xiaoqian Jiang (University of Texas - Health, USA), and Amalio Telenti (Scripps Institute, USA)

RAI4IoE: Responsible AI for Enabling the Internet of Energy 13
Minhui Xue (CSIRO's Data61, Australia), Surya Nepal (CSIRO's Data61, Australia), Ling Liu (Georgia Institute of Technology, USA), 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, Australia)

Synthetic Information and Digital Twins for Pandemic Science: Challenges and Opportunities..... 23
Galen Harrison (University of Virginia, VA), Przemyslaw Porebski (University of Virginia, VA), Jiangzhuo Chen (University of Virginia, VA), Mandy Wilson (University of Virginia, VA), Henning Mortveit (University of Virginia, VA), Parantapa Bhattacharya (University of Virginia, VA), Dawen Xie (University of Virginia, VA), Stefan Hoops (University of Virginia, VA), Anil Vullikanti (University of Virginia, VA), Li Xiong (Emory University, GA), James Joshi (University of Pittsburgh, PA), and Madhav Marathe (University of Virginia, VA)

Supporting Pandemic Preparedness with Privacy Enhancing Technology 34
Ruixuan Liu (Emory University), Sepanta Zeighami (University of Southern California), Haowen Lin (University of Southern California), Cyrus Shahabi (University of Southern California), Yang Cao (Hokkaido University), Shun Takagi (Kyoto University), Yoko Konishi (Kochi University), Masatoshi Yoshikawa (Osaka Seikei University), and Li Xiong (Emory University)

Preserving Location Privacy in the Modern Era of Pervasive Environments 44
Tyler Nicewaner (Vanderbilt University, USA), Alian Yu (Vanderbilt University, USA), Wei Jiang (Oracle Labs, USA), and Dan Lin (Vanderbilt University, USA)

Web 3.0 and the Ownership of Learning 52
Sarah A. Flanery (Texas A&M University, USA), Christiana Chamon (Texas A&M University, USA), Srujan D. Kotikela (Texas A&M University–Commerce, USA), and Francis K. Quek (Texas A&M University, USA)

Research: Security and Privacy in AI and IoT

FUBA: Federated Uncovering of Backdoor Attacks for Heterogeneous Data 55
Fabiola Espinoza Castellon (Institut LIST, CEA, Universite Paris-Saclay, France), Deepika Singh (Institut LIST, CEA, Universite Paris-Saclay, France), Aurélien Mayoue (Institut LIST, CEA, Universite Paris-Saclay, France), and Cédric Gouy-Pailler (Institut LIST, CEA, Universite Paris-Saclay, France)

Learnable Image Transformations for Privacy Enhanced Deep Neural Networks 64
David Rodriguez (University of Texas at San Antonio, USA) and Ram Krishnan (University of Texas at San Antonio, USA)

Metamorphic Malware Evolution: The Potential and Peril of Large Language Models 74
Pooria Madani (Ontario Tech University, Canada)

A Privacy-Preserving Framework for Collaborative Machine Learning with Kernel Methods 82
Anika Hannemann (Leipzig University, Germany), Ali Burak Ünal (University of Tübingen, Germany), Arjhun Swaminathan (University of Tübingen, Germany), Erik Buchmann (Leipzig University, Germany), and Mete Akgün (University of Tübingen, Germany)

Mitigating Targeted Universal Adversarial Attacks on Time Series Power Quality Disturbances Models 91
Sultan Uddin Khan (North Carolina A&T State University, USA), Mohammed Mynuddin (North Carolina A&T State University, USA), Isaac Adom (North Carolina A&T State University, USA), and Mahmoud Nabil Mahmoud (North Carolina A&T State University, USA)

Resource-Efficient and Data Type-Aware Authentication Protocol for Internet of Things Systems 101
Cong Pu (Oklahoma State University, USA), Imtiaz Ahmed (Howard University, USA), and Sumit Chakravarty (Kennesaw State University, USA)

Vision/Research: Trust and Privacy II

Trust, Privacy and Security Aspects of Bias and Fairness in Machine Learning 111
Asli Atabek (Koç University, Turkey), Egehan Eralp (Koç University, Turkey), and M. Emre Gursoy (Koç University, Turkey)

Centering Policy and Practice: Research Gaps Around Usable Differential Privacy 122
Rachel Cummings (Columbia University, USA) and Jayshree Sarathy (Columbia University, USA)

ForensiBlock: A Provenance-Driven Blockchain Framework for Data Forensics and Auditability.... 136
Asma Jodeiri Akbarfam (Augusta University, USA), Mahdieh Heidaripour (Augusta University, USA), Hoda Maleki (Augusta University, USA), Gokila Dorai (Augusta University, USA), and Gagan Agrawal (University of Georgia, USA)

Seamless Asset Exchange in Interconnected Metaverses: Unraveling On-Chain Atomic Swap 146
Shakila Zaman (University of North Texas, USA), Ram Dantu (University of North Texas, USA), Syed Badruddoja (California State University, USA), Sirisha Talapuru (University of North Texas, USA), and Kritagya Upadhyay (Middle Tennessee SU, USA)

Revisit Linear Transformation for Image Privacy in Machine Learning 156
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 FL 163
Mohammed Alduniawi (Florida International University, USA), Kemal Akkaya (Florida International University, USA), and Ruimin Sun (Florida International University, USA)

Vision: AI/LLM Security and Explainability

An Investigation on the Fragility of Graph Neural Networks: the Impact of Node Feature Modification on Graph Classification Accuracy 169
Chengen Wang (University of Texas at Dallas), Yan Zhou (University of Texas at Dallas), Kangkook Jee (University of Texas at Dallas), and Murat Kantarcioglu (University of Texas at Dallas)

Towards Neuro-Symbolic AI for Assured and Trustworthy Human-Autonomy Teaming 177
Danda B.Rawat (Howard University, Washington)

Secure Multimedia Data Systems in the Era of Artificial Intelligence: Significant Progress and Vision for the Future 180
Bhavani Thuraisingham (The University of Texas at Dallas)

Explainable AI for Prioritizing and Deploying Defenses for Cyber-Physical System Resiliency 184
Indrajit Ray (Colorado State University, USA), Sarath Sreedharan (Colorado State University, USA), Rakesh Podder (Colorado State University, USA), Shadaab Kawnain Bashir (Colorado State University, USA), and Indrakshi Ray (Colorado State University, USA)

Invisible Watermarking for Audio Generation Diffusion Models 193
Xirong Cao (Fordham University, USA), Xiang Li (Fordham University, USA), Divyesh Jadav (IBM Research, USA), Yanzhao Wu (Florida International University, USA), Zhehui Chen (Google, USA), Chen Zeng (Google, USA), and Wenqi Wei (Fordham University, USA)

Model Based Risk Assessment and Risk Mitigation Framework for Cyber-Physical Systems 203
Shwetha Gowdanakatte (Colorado State University, USA), Indrakshi Ray (Colorado State University, USA), and Mahmoud Abdelgawad (Colorado State University, USA)

Research: Blockchain, Access Control and Privacy

Mind the CORS 213
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 222
Reginald Cushing (Netherlands eScience Center, Netherlands), Xin Zhou (University of Amsterdam, Netherlands), Adam Belloum (Netherlands eScience Center; 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 230
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 240
Adam Beauchaine (Worcester Polytechnic Institute, USA) and Craig A. Shue (Worcester Polytechnic Institute, USA)

Ensuring Privacy Policy Compliance of Wearables with IoT Regulations 247
Kelvin Uzoma Echenim (University of Maryland Baltimore County, USA), Lavanya Elluri (Texas A&M University - Central Texas, USA), and Karuna Pande Joshi (University of Maryland Baltimore County, USA)

Balancing Privacy and Accuracy in IoT Using Domain-Specific Features for Time Series Classification 257
Pranshul Lakhanpal (California Polytechnic State University, USA), Asmita Sharma (California Polytechnic State University, USA), Joydeep Mukherjee (California Polytechnic State University, USA), Marin Litoiu (York University, Canada), and Sumona Mukhopadhyay (California Polytechnic State University, USA)

Vision: Security and Trust in LLMs, Iot and Metaverse

Beyond Basic Trust: Envisioning the Future of NextGen Networked Systems and Digital Signatures 267
Attila A. Yavuz (University of South Florida, USA), Kiarash Sedghighadikolaei (University of South Florida, USA), Saleh Darzi (University of South Florida, USA), and Saif E. Nouma (University of South Florida, USA)

Digital Twins and the Future of Their Use Enabling Shift Left and Shift Right Cybersecurity Operations 277
Ahmad Mohsin (Security Research Institute (SRI); Cyber Security Cooperative Research Centre (CSCRC), Australia), Helge Janicke (Security Research Institute (SRI); Cyber Security Cooperative Research Centre (CSCRC), Australia), Surya Nepal (Data61, CSIRO, Australia), and David Holmes (Security Research Institute (SRI); Cyber Security Cooperative Research Centre (CSCRC), Australia)

The Dark Side of the Metaverse: Why is it Falling Short of Expectations? 287
Sirisha Talapuru (University of North Texas, USA), Ram Dantu (University of North Texas, USA), Kritagya Upadhyay (Middle Tennessee State University, USA), Syed Badruddoja (California State University, USA), and Shakila Zaman (University of North Texas, USA)

Large Language Model-Powered Smart Contract Vulnerability Detection: New Perspectives 297
Sihao Hu (Georgia Institute of Technology, USA), Tiansheng Huang (Georgia Institute of Technology, USA), Fatih İlhan (Georgia Institute of Technology, USA), Selim Furkan Tekin (Georgia Institute of Technology, USA), and Ling Liu (Georgia Institute of Technology, USA)

Large Language Models and Computer Security 307
Arun Iyengar (Cisco Research) and Ashish Kundu (Cisco Research)

Research: Security and Privacy

k-Anonymity in Federated Heterogenous Graphs and k-Core Anonymization 314
Mark Dockendorf (University of North Texas, USA) and Ram Dantu (University of North Texas, USA)

Performance Analysis of Homomorphically-Encrypted Heterogeneous Multi-Layer Graph Databases. 324
John Long (University of North Texas, USA), Ram Dantu (University of North Texas, USA), and Jacob White (University of North Texas, USA)

Harvesting Security: A Semantically Enriched Access Control Architecture for Smart Farms 335
Ghadeer I Yassin (University of Georgia, USA) and Lakshmish Ramaswamy (University of Georgia, USA)

Peculiarity and Diversity Measures to Evaluate Attribute-Based Access Rules 344
Abner Perez-Haro (CINVESTAV, Mexico) and Arturo Diaz-Perez (CINVESTAV, Mexico)

Quantitative Risk Analysis With Qualitative Statements 350
Karim Elhammady (University of Waterloo, Canada) and Sebastian Fischmeister (University of Waterloo, Canada)

Industry Session

A Comprehensive Analysis of Trust, Privacy, and Security Measures in the Digital Age 360
Debashis Das (Narula Institute of Technology, India), Sourav Banerjee (Kalyani Government Engineering College, India), Pushpita Chatterjee (Howard University, USA), and Uttam Ghosh (Meharry Medical College, USA)

Secured Data Movement Using Data Ring Fencing 370
Aditya Nangia (IIIT Delhi, India), Saksham Bhupal (IIIT Delhi, India), Mukesh Mohania (IIIT Delhi, India), and Chinmay Kundu (KIIT University, India)

The Effect of Human v/s Synthetic Test Data and Round-Tripping on Assessment of Sentiment Analysis Systems for Bias 380
Kausik Lakkaraju (University of South Carolina, USA), Aniket Gupta (Netaji Subhas University of Technology, India), Biplav Srivastava (University of South Carolina, USA), Marco Valtorta (University of South Carolina, USA), and Dezhi Wu (University of South Carolina, USA)

CRISP: Change Risk for IT Service Providers 390
Arun Ayachitula (n/a) and Upendra Sharma (n/a)

SOC and Academia – Building Resilient Systems 396
Carson Zimmerman (Microsoft Corporation) and Abhilasha Bhargav-Spantzel (Microsoft Corporation)

Bridging the Gap: Industry Perspectives and Trends in Cloud Security, and Opportunities for Collaborative Research 400
Sarabjeet Chugh (Cisco Systems, Inc., USA)

Author Index **405**