2022 IEEE 4th International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications (TPS-ISA 2022)

Virtual Conference
14-17 December 2022

IEEE Catalog Number: CFP22V08-POD
ISBN: 978-1-6654-7409-2

**Copyright © 2022 by the Institute of Electrical and Electronics Engineers, Inc.
All Rights Reserved**

Copyright and Reprint Permissions: Abstracting is permitted with credit to the source. Libraries are permitted to photocopy beyond the limit of U.S. copyright law for private use of patrons those articles in this volume that carry a code at the bottom of the first page, provided the per-copy fee indicated in the code is paid through Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923.

For other copying, reprint or republication permission, write to IEEE Copyrights Manager, IEEE Service Center, 445 Hoes Lane, Piscataway, NJ 08854. All rights reserved.

****** 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:	CFP22V08-POD
ISBN (Print-On-Demand):	978-1-6654-7409-2
ISBN (Online):	978-1-6654-7408-5

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

CURRAN ASSOCIATES INC.
proceedings
.com

2022 IEEE 4th International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications (TPS-ISA)

TPS-ISA 2022

Table of Contents

Message from the General Chairs and PC Chairs x
Organizing Committee xii
Technical Program Committee xiii
Steering Committee xiv
Keynotes xv
Plenary Panel xvii

TPS Vision Session 1

Privacy and Security Issues for Human Digital Twins 1
Giorgia Sirigu (University of Insubria, Italy), Barbara Carminati (University of Insubria, Italy), and Elena Ferrari (University of Insubria, Italy)

A Universal Deduplication Architecture for Secure and Efficient Cloud Storage 10
Kevin Saric (QUT, CSIRO Data61, CSCRC, Australia), Gowri Sankar Ramachandran (Queensland University of Technology, Australia), Shantanu Pal (Deakin University, Australia), Raja Jurdak (Queensland University of Technology, Australia), and Surya Nepal (CSIRO Data61, CSCRC, Australia)

Accountable AI for Healthcare IoT Systems 20
Prachi Bagave (Delft University of Technology, The Netherlands), Marcus Westberg (Delft University of Technology, The Netherlands), Roel Dobbe (Delft University of Technology, The Netherlands), Marijn Janssen (Delft University of Technology), and Aaron Yi Ding (Delft University of Technology, The Netherlands)

Distributed Cyber-Infrastructures and Artificial Intelligence in Hybrid Post-Quantum Era 29
Attila A. Yavuz (University of South Florida, USA), Saif E. Nouma (University of South Florida, USA), Thang Hoang (Virginia Tech, USA), Duncan Earl (Qubitekk, Inc, USA), and Scott Packard (Qubitekk, Inc., USA)

TPS Vision Session 2

Auditing Metaverse Requires Multimodal Deep Learning 39
Kritagya Upadhyay (University of North Texas, USA), Ram Dantu (University of North Texas, USA), Yanyan He (University of North Texas, USA), Syed Badruddoja (University of North Texas, USA), and Abiola Salau (University of North Texas, USA)

Developing Self-Evolving Deepfake Detectors Against AI Attacks 47
Ian Miller (Vanderbilt University, USA) and Dan Lin (Vanderbilt University, USA)

Privacy Challenges and Solutions for Image Data Sharing 55
Liyue Fan (University of North Carolina at Charlotte, USA)

TPS Research Session 1

Maintaining Review Credibility using NLP, Reputation, and Blockchain 58
Zachary Zaccagni (University of North Texas, USA), Ram Dantu (University of North Texas, USA), and Kirill Morozov (University of North Texas, USA)

MnemoSys: A Conditional Probability Estimation Protocol for Blockchain Audited Reputation Management 67
Daniel Rouhana (Washington State University), Peyton Lundquist (Boise State University), Tim Andersen (Boise State University), and Gaby G. Dagher (Boise State University)

Managing Reputation Scores in a Blockchain-Based Decentralized Marketplace 77
Ravi Mukkamala (Old Dominion University, USA), Stephan Olariu (Old Dominion University, USA), Meshari Aljohani (Old Dominion University, USA), and Sandeep Kalari (Old Dominion University, USA)

Efficient Blockchain Enabled Attribute-Based Access Control as a Service 87
Ritik Kumar (Indian Institute of Technology Kharagpur, India), Balaji Palanisamy (University of Pittsburgh, USA), and Shamik Sural (Indian Institute of Technology Kharagpur, India)

TPS Research Session 2

Money Talks: Detection of Disposable Phishing Websites by Analyzing Its Building Costs 97
Daiki Ito (Deloitte Tohmatsu Cyber LLC, Japan), Yuta Takata (Deloitte Tohmatsu Cyber LLC, Japan), and Masaki Kamizono (Deloitte Tohmatsu Cyber LLC, Japan)

Investigating Organizational Factors Associated with GDPR Noncompliance using Privacy Policies: A Machine Learning Approach 107
Abdel-Jaouad Aberkane (Ghent University, Belgium), Seppe Vanden Broucke (Ghent University, Belgium), and Geert Poels (Ghent University, Belgium)

Enabling Location Based Services with Privacy and Integrity Protection in Untrusted Environments Through Blockchain and Secure Computation 114
Michele Amoretti (University of Parma, Italy), Alexandru Budianu (ESA/ESTEC, Netherlands), Gianluca Caparra (ESA/ESTEC, Netherlands), Felice D'Agruma (University of Parma, Italy), Davide Ferrari (University of Parma, Italy), Gabriele Penzotti (University of Parma, Italy), Luca Veltri (University of Parma, Italy), and Francesco Zanichelli (University of Parma, Italy)

A Method of Constructing Malware Classification Dataset using Clustering 124
Woo-Jin Joe (Chungnam National University, Korea) and Hyong-Shik Kim (Chungnam National University, Korea)

TPS Research Session 3

Detecting Cloud-Based Phishing Attacks by Combining Deep Learning Models 130
Birendra Jha (Eydle Inc.), Medha Atre (Eydle Inc.), and Ashwini Rao (Eydle Inc.)

ML-FEED: Machine Learning Framework for Efficient Exploit Detection 140
Tanujay Saha (Princeton University), Tamjid Al-Rahat (University of California, Los Angeles, USA), Najwa Aaraj (Technology Innovation Institute, Abu Dhabi, United Arab Emirates), Yuan Tian (University of California, Los Angeles, USA), and Niraj K. Jha (Princeton University, USA)

Impact of Dimensionality Reduction on Outlier Detection: an Empirical Study 150
Vivek Vaidya (East Brunswick High School, USA) and Jaideep Vaidya (Rutgers University, USA)

Weaponizing IoT Sensors: When Table Choice Poses a Security Vulnerability 160
Gustavo Casqueiro (Military Institute of Engineering, Brasil), Sayed Erfan Arefin (Texas Tech University, USA), Tasnia Ashrafi Heya (Texas Tech University, USA), Abdul Serwadda (Texas Tech University, USA), and Hassan Wasswa (Texas Tech University, USA)

TPS Research Session 4

Resilience of Wireless Ad Hoc Federated Learning Against Model Poisoning Attacks 168
Naoya Tezuka (The University of Tokyo), Hideya Ochiai (The University of Tokyo), Yuwei Sun (The University of Tokyo), and Hiroshi Esaki (The University of Tokyo)

Beta Poisoning Attacks Against Machine Learning Models: Extensions, Limitations and Defenses 178
Atakan Kara (Koc University, Turkey), Nursena Koprucu (Koc University, Turkey), and M. Emre Gursoy (Koc University, Turkey)

Enhanced Scanning in SDN Networks and its Detection using Machine Learning 188
Abdullah H. Alqahtani (The University of Sheffield, United Kingdom) and John A. Clark (The University of Sheffield, United Kingdom)

Defending Against Targeted Poisoning Attacks in Federated Learning 198
Pinar Erbil (Koc University, Turkey) and M. Emre Gursoy (Koc University, Turkey)

TPS Research Session 5

Secure and Efficient Privacy-Preserving Authentication Scheme using Cuckoo Filter in Remote Patient Monitoring Network 208
Shafika Showkat Moni (Montclair State University, Montclair, New Jersey, USA) and Deepti Gupta (University of Texas at San Antonio, San Antonio, Texas, USA)

Scenario-Driven Device-to-Device Access Control in Smart Home IoT 217
Mehrnoosh Shakarami (University of Texas at San Antonio, USA), James Benson (University of Texas at San Antonio, USA), and Ravi Sandhu (University of Texas at San Antonio, USA)

Harpocrates: Privacy-Preserving and Immutable Audit Log for Sensitive Data Operations 229
Mohit Bhasi Thazhath (Virginia Tech, USA), Jan Michalak (Virginia Tech, USA), and Thang Hoang (Virginia Tech, USA)

Adaptive Control for Security and Resilience of Networked Cyber-Physical Systems: Where Are We? 239
Talal Halabi (Laval University, Canada), Israat Haque (Dalhousie University, Canada), and Hadis Karimipour (University of Calgary, Canada)

TPS Research Session 6

ZAC: Efficient Zero-Knowledge Dynamic Universal Accumulator and Application to Zero-Knowledge Elementary Database 248
Hai-Van Dang (University of Plymouth), Tran Viet Xuan Phuong (School of Cybersecurity, Old Dominion University), Thuc D. Nguyen (University of Science, VNU-HCM), and Thang Hoang (Virginia Tech)

What Makefile? Detecting Compiler Information Without Source using The Code Property Graph. 258
Sean Deaton (Blue Star and Bogart Associates, USA)

ProProv: A Language and Graphical Tool for Specifying Data Provenance Policies 266
Kevin Dennis (University of South Florida, USA), Shamaria Engram (MIT Lincoln Laboratory, USA), Tyler Kaczmarek (MIT Lincoln Laboratory, USA), and Jay Ligatti (University of South Florida, USA)

TPS Special Session on AI Security

Dynamic Defenses and the Transferability of Adversarial Examples 276
Sam Thomas (East Carolina University, USA), Farnoosh Koleini (East Carolina University, USA), and Nasseh Tabrizi (East Carolina University, USA)

Understanding Model Extraction Games 285
Xun Xian (University of Minnesota, USA), Mingyi Hong (University of Minnesota, USA), and Jie Ding (University of Minnesota, USA)

TPS Special Session on Blockchain

Towards Faster Settlement in HTLC-Based Cross-Chain Atomic Swaps 295
Subhra Mazumdar (TU Wien, Christian Doppler Laboratory Blockchain Technologies for the Internet of Things Vienna, Austria)

Last Mile of Blockchains: RPC and Node-as-a-service 305
Zhongtang Luo (Purdue University), Rohan Murukutla (Supra), and Aniket Kate (Purdue University; Supra)

Author Index **313**