2024 IEEE 6th International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications (TPS-ISA 2024)

Washington, DC, USA
28-31 October 2024

IEEE Catalog Number: CFP24V08-POD
ISBN: 979-8-3503-8675-2

****** 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: CFP24V08-POD
ISBN (Print-On-Demand): 979-8-3503-8675-2
ISBN (Online): 979-8-3503-8674-5

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

2024 IEEE 6th International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications (TPS-ISA)

TPS-ISA 2024

Table of Contents

Message from the General Chairs and PC Chairs ..... **xiv**
Steering Committee ..... **xvi**
Organizing Committee ..... **xvii**
Technical Program Committee ..... **xviii**
Keynotes ..... **xx**
Plenary Panel ..... **xxii**

Malware Detection, Forensics, and Deep Learning

Large Language Models to Enhance Malware Detection in Edge Computing 1
Christian Rondanini (University of Insubria, Italy), Barbara Carminati (University of Insubria, Italy), Elena Ferrari (University of Insubria, Italy), Ashish Kundu (Cisco Research, USA), and Akshay Jajoo (Cisco Research, USA)

Digital Evidence Chain of Custody: Navigating New Realities of Digital Forensics 11
Souradip Nath (Arizona State University, USA), Keb Summers (Arizona State University, USA), Jaejong Baek (Arizona State University, USA), and Gail-Joon Ahn (Arizona State University, USA)

Boosting Imperceptibility of Stable Diffusion-Based Adversarial Examples Generation with Momentum 21
Nashrah Haque (Fordham University, USA), Xiang Li (Fordham University, USA), Zhehui Chen (Google, USA), Yanzhao Wu (Florida International University, USA), Lei Yu (Rensselaer Polytechnic Institute, USA), Arun Iyengar (Cisco Research, USA), and Wenqi Wei (Fordham University, USA)

Privacy Enhancing Technologies and Cybersecurity Threats

Distributed, Privacy-Aware Location Data Aggregation 31
Maja Schneider (Center for Scalable Data Analytics and Artificial Intelligence (ScaDS.AI), Germany), Erik Buchmann (Center for Scalable Data Analytics and Artificial Intelligence (ScaDS.AI), Germany), and Erhard Rahm (Center for Scalable Data Analytics and Artificial Intelligence (ScaDS.AI), Germany)

Utility-Privacy Aware Mobile Diminished Reality Framework for 3D Visual Privacy 41
Salam Tabet (American University of Beirut, Lebanon), Ayman Kayssi (American University of Beirut, Lebanon), and Imad H. Elhajj (American University of Beirut, Lebanon)

A Privacy-Preserving Cyber Threat Intelligence Sharing System 49
Philip Huff (University of Arkansas, USA), Spencer Massengale (University of Arkansas, USA), Tran Viet Xuan Phuong (University of Arkansas, USA), and Sri Nikhil Gupta Gourisetti (University of Arkansas, USA)

Improved Ethereum Fraud Detection Mechanism with Explainable Tabular Transformer Model 59
Ruth Olusegun (Bowie State University, USA) and Bo Yang (Bowie State University, USA)

Unsupervised Approach for Electricity Theft Detection Combining Recurrent Neural Networks and Rule-Based Policy 69
Ashley Ajuz (University of Pittsburgh, PA) and Mai Abdelhakim (University of Pittsburgh, PA)

Large Language Models for Privacy and Security

Bias Detection and Mitigation in Zero-Shot Spam Classification Using LLMs 77
Hossein Salemi (George Mason University, USA), Anuridhi Gupta (George Mason University, USA), and Hemant Purohit (George Mason University, USA)

Towards Transparent Intrusion Detection: A Coherence-Based Framework in Explainable AI Integrating Large Language Models 87
Areej Alnahdi (University of Massachusetts Lowell, USA) and Sashank Narain (University of Massachusetts Lowell, USA)

PrivComp-KG: Leveraging KG and LLM for Compliance Verification 97
Leon Garza (The University of Texas at El Paso, USA), Lavanya Elluri (Texas A&M University Central Texas, USA), Aritran Piplai (The University of Texas at El Paso, USA), Anantaa Kotal (The University of Texas at El Paso, USA), Deepti Gupta (Texas A&M University Central Texas, USA), and Anupam Joshi (University of Maryland Baltimore County, USA)

A Qualitative Study on Using ChatGPT for Software Security: Perception vs. Practicality 107
M. Mehdi Kholoosi (The University of Adelaide, Australia; Cyber Security Cooperative Research Centre, Australia), M. Ali Babar (The University of Adelaide, Australia; Cyber Security Cooperative Research Centre, Australia), and Roland Croft (The University of Adelaide, Australia; Cyber Security Cooperative Research Centre, Australia)

Automated Consistency Analysis of LLMs 118
Aditya Patwardhan (Stony Brook University, USA), Vivek Vaidya (Rutgers University, USA), and Ashish Kundu (Cisco Research, USA)

Bridging the Legal Divide: Contractual Enforceability and Acceptability in the AI-Driven Automated Conversion of Smart Legal Contracts 128
Shriyaa Balaji (University of North Texas, USA), Ram Dantu (University of North Texas, USA), Kritagya Upadhyay (Middle Tennessee State University, USA), and Thomas McCullough (University of North Texas, USA)

AI, Quantum Computing, and Cybersecurity

Counter Denial of Service for Next-Generation Networks Within the Artificial Intelligence and Post-Quantum Era 138
Saleh Darzi (University of South Florida, USA) and Attila Yavuz (University of South Florida, USA)

Federated Learning in Practice: Reflections and Projections 148
Katharine Daly (Google Research), Hubert Eichner (Google Research), Peter Kairouz (Google Research), H. Brendan McMahan (Google Research), Daniel Ramage (Google Research), and Zheng Xu (Google Research)

Privacy in Practice: Research Challenges in the Deployment of Privacy-Preserving ML 157
Stacey Truex (Denison University, USA) and Margaret Malan (Denison University, USA)

ZCube: A Zero-Trust, Zero-Knowledge, and Zero-Memory Platform for Privacy and yet Secured Access 166
Vinh Quach (University of North Texas, USA), Ram Dantu (University of North Texas, USA), Sirisha Talapuru (University of North Texas, USA), Shakila Zaman (University of North Texas, USA), and Apurba Pokharel (University of North Texas, USA)

The Intersection of Quantum Computing, AI, and Cybersecurity: Challenges and Opportunities.... 176
Danda Rawat (Howard University, USA) and Chandra Bajracharya (University of Maryland Global Campus, USA)

Privacy and Security in AI/ML

Dynamic Black-box Backdoor Attacks on IoT Sensory Data 182
Ajesh Koyatan Chathoth (University of Pittsburgh, USA) and Stephen Lee (University of Pittsburgh, USA)

Resilient Federated Learning Using Trimmed-Clipping Aggregation 192
Chandreyee Bhowmick (Vanderbilt University) and Xenofon Koutsoukos (Vanderbilt University)

Noise as a Double-Edged Sword: Reinforcement Learning Exploits Randomized Defenses in Neural Networks 202
Steve Bakos (Ontario Tech University, Canada), Pooria Madani (Ontario Tech University, Canada), and Heidar Davoudi (Ontario Tech University, Canada)

Preserving Privacy During Reinforcement Learning With AI Feedback 211
David Gao (Vanderbilt University), Ian Miller (Vanderbilt University), Ali Allami (Vanderbilt University), and Dan Lin (Vanderbilt University)

Towards Assessing Integrated Differential Privacy and Fairness Mechanisms in Supervised Learning 221
Maryam Aldairi (University of Pittsburgh, King Faisal University) and James Joshi (Universit of Pittsburgh)

MOFHEI: Model Optimizing Framework for Fast and Efficient Homomorphically Encrypted Neural Network Inference 233
Parsa Ghazvinian (Georgia State University), Robert Podschwadt (Old Dominion University), Prajwal Panzade (Georgia State University), Mohammad H. Rafiei (Johns Hopkins University), and Daniel Takabi (Old Dominion University)

AI Security, Privacy, and Healthcare

LLM-Sentry: A Model-Agnostic Human-in-the-Loop Framework for Securing Large Language Models 245
Saquib Irtiza (University of Texas at Dallas, USA), Khandakar Ashrafi Akbar (University of Texas at Dallas, USA), Arowa Yasmeen (University of Texas at Dallas, USA), Latifur Khan (University of Texas at Dallas, USA), Ovidiu Daescu (University of Texas at Dallas, USA), and Bhavani Thuraisingham (University of Texas at Dallas, USA)

PrivacySphere: Privacy-Preserving Smart Spaces 255
Habiba Farrukh (University of California, Irvine), Nada Lahjouji (University of California, Irvine), Sharad Mehrotra (University of California, Irvine), Faisal Nawab (University of California, Irvine), Julie Rousseau (University of California, Irvine), Shantanu Sharma (New Jersey Institute of Technology), Nalini Venkatasubramanian (University of California, Irvine), and Roberto Yus (University of Maryland, Baltimore County)

Patient-Centered and Practical Privacy to Support AI for Healthcare 265
Ruixuan Liu (Emory University, USA), Hong Kyu Lee (Emory University, USA), Sivasubramanium V Bhavani (Emory University, USA), Xiaoqian Jiang (UTHealth Houston, USA), Lucila Ohno-Machado (Yale University, USA), and Li Xiong (Emory University, USA)

Advances in Privacy Preserving Federated Learning to Realize a Truly Learning Healthcare System 273
Ravi Madduri (Argonne National Laboratory, USA), Zilinghan Li (Argonne National Laboratory, USA), Tarak Nandi (Argonne National Laboratory, USA), Kibaek Kim (Argonne National Laboratory, USA), Minseok Ryu (Arizona State University, USA), and Alexis Rodriguez (Argonne National Laboratory, USA)

Towards Privacy-Preserving and Secure Machine Unlearning: Taxonomy, Challenges and Research Directions 280
Liou Tang (University of Pittsburgh, USA) and James Joshi (University of Pittsburgh, USA)

Malware and Threat Detection

Resiliency Graphs: Modelling the Interplay Between Cyber Attacks and System Failures Through AI Planning 292
Shadaab Kawnain Bashir (Colorado State University, USA), Rakesh Podder (Colorado State University, USA), Sarath Sreedharan (Colorado State University, USA), Indrakshi Ray (Colorado State University, USA), and Indrajit Ray (Colorado State University, USA)

SR2ACM: A Methodical Approach for Translating Natural Language Security Requirements to Access Control Model 303
Saja Alqurashi (Colorado State University, USA), Indrakshi Ray (Colorado State University, USA), Mahmoud Abdelgawad (Colorado State University, USA), and Hossein Shirazi (San Diego State University, USA)

Fine-Tuning LLMs for Code Mutation: A New Era of Cyber Threats 313
Mohammad Setak (Ontario Tech University, Canada) and Pooria Madani (Ontario Tech University, Canada)

HAL 9000: a Risk Manager for ITSs 322
Tadeu Freitas (University of Porto, Portugal; CRACS/INESC-TEC, Portugal), Carlos Novo (University of Porto, Portugal), João Soares (University of Porto, Portugal; CRACS/INESC-TEC, Portugal), Inês Dutra (University of Porto, Portugal; CINTESIS@RISE, Portugal), Manuel Correia (University of Porto, Portugal; CRACS/INESC-TEC, Portugal), Behnam Shariati (University of Maryland, USA), and Rolando Martins (University of Porto, Portugal; SafeHelm, Portugal)

Discovery of Evolving Relationships of Software Vulnerabilities 332
Hailey Sparks (College of Charleston, USA) and Krishnendu Ghosh (College of Charleston, USA)

Leveraging Multimodal Retrieval-Augmented Generation for Cyber Attack Detection in Transit Systems 341
Muhaimin Bin Munir (The University of Texas, USA), Yuchen Cai (The University of Texas, USA), Latifur Khan (The University of Texas, USA), and Bhavani Thuraisingham (The University of Texas, USA)

Access Control and Security Models

BobGAT: Towards Inferring Software Bill of Behavior with Pre-Trained Graph Attention Networks 351
Justin Allen (Lawrence Livermore National Lab, USA) and Geoff Sanders (Lawrence Livermore National Lab, USA)

Translating Natural Language Specifications into Access Control Policies by Leveraging Large Language Models 361
Sherifdeen Lawal (University of Texas at San Antonio, USA), Xingmeng Zhao (University of Texas at San Antonio, USA), Anthony Rios (University of Texas at San Antonio, USA), Ram Krishnan (University of Texas at San Antonio, USA), and David Ferraiolo (National Institute of Standards and Technology, USA)

Constraints Visualization and Specification for Activity-Centric Access Control 371
Tanjila Mawla (Tennessee Tech University, USA) and Maanak Gupta (Tennessee Tech University, USA)

Fast and Post-Quantum Authentication for Real-Time Next Generation Networks with Bloom Filter 381
Kiarash Sedghighadikolaei (University of South Florida, USA) and Attila A Yavuz (University of South Florida, USA)

Secure Cross-Chain Provenance for Digital Forensics Collaboration 389
Asma Jodeiri Akbarfam (Augusta University, USA), Gokila Dorai (Augusta University, USA), and Hoda Maleki (Augusta University, USA)

Genesis of Cyber Threats: Towards Malware-Based Advanced Persistent Threat (APT) Attribution 399
Nanda Rani (Indian Institute of Technology Kanpur, India), Bikash Saha (Indian Institute of Technology Kanpur, India), Ravi Kumar (C3ihub, IIT Kanpur, India), and Sandeep Kumar Shukla (Indian Institute of Technology Kanpur, India)

Workshop LLM CyberSec Agenda

Paper Session 1

[Short Paper] Forensic Analysis of Indirect Prompt Injection Attacks on LLM Agents 409
Maxim Chernyshev (Deakin University, Australia), Zubair Baig (Deakin University, Australia), and Robin Doss (Deakin University, Australia)

Pitfalls of Generic Large Language Models (GLLMs) from Reliability and Security Perspectives 412
Dipankar Dasgupta (The University of Memphis, USA) and Arunava Roy (The University of Memphis, USA)

Paper Session 2

Large Language Models for Hardware Security (Invited, Short Paper) 420
Hammond Pearce (University of New South Wales) and Benjamin Tan (University of Calgary)

Short Paper: Secure Lightweight Computation for Federated N-Gram Language Model 424
Tho Thi Ngoc Le (HUTECH University, Vietnam) and Tran Viet Xuan Phuong (University of Arkansas at Little Rock, USA)

Probing Robustness of In-Context Learning in LLM Classification Predictions Under Label Noise 427
Sriya Ayachitula (Ardsley High School, USA), Chinmay Kundu (Kiit University, INDIA), and Birendra Mishra (University of California, USA)

Workshop Inclusive AI for Cybersecurity Agenda

Paper Session 1

Design Challenges for Scam Prevention Tools to Protect Neurodiverse and Older Adult Populations 437
Pragathi Tummala (George Mason University, USA), Hannah Choi (George Mason University, USA), Anuridhi Gupta (George Mason University, USA), Tomas A Lapnas (George Mason University, USA), Yoo Sun Chung (George Mason University, USA), Matthew Peterson (George Mason University, USA), Geraldine Walther (George Mason University, USA), and Hemant Purohit (George Mason University, USA)

Towards Inclusive Cybersecurity: Protecting the Vulnerable with Social Cyber Vulnerability Metrics 442
Shutonu Mitra (Virginia Tech, USA), Qi Zhang (Virginia Tech, USA), Chen-Wei Chang (Virginia Tech, USA), Hossein Salemi (George Mason University, USA), Hemant Purohit (George Mason University, USA), Fengxiu Zhang (George Mason University, USA), Michin Hong (Indiana University, USA), Chang-Tien Lu (Virginia Tech, USA), and Jin-Hee Cho (Virginia Tech, USA)

A Blockchain-Enabled Approach to Cross-Border Compliance and Trust 446
Vikram Kulothungan (Capitol Technology University, USA)

Mind the Inclusion Gap: A Critical Review of Accessibility in Anti-Counterfeiting Technologies 455
Krishna Purohit (George Mason University, USA), Salem Abdul-Baki (George Mason University, USA), and Hemant Purohit (George Mason University, USA)

Workshop QUILLS

Quantum Computing & Algorithms

Randomized Benchmarking of Local Zeroth-Order Optimizers for Variational Quantum Systems .. 461
Lucas Tecot (University of California, USA) and Cho-Jui Hsieh (University of California, USA)

Pragmatic Obfuscation of Factoring in Hamiltonian Simulation and Ground State Estimation 471
Dhruv Gopalakrishnan (University of Waterloo, Canada) and Michele Mosca (University of Waterloo, Canada)

Study of Attacks on the HHL Quantum Algorithm 481
Yizhuo Tan (Yale University, USA), Hrvoje Kukina (TU Wien, Austria), and Jakub Szefer (Yale University, USA)

Synergizing Error Suppression, Mitigation and Correction for Fault-Tolerant Quantum Computing 489
Yanzhang Zhu (University of Central Florida, USA), Siyuan Niu (University of Central Florida, USA; Lawrence Berkeley National Laboratory, USA), and Di Wu (University of Central Florida, USA)

Quantum Services with Efficiency and Privacy

Simulation of Quantum Homomorphic Encryption: Demonstration and Analysis 491
Sohrab Ganjian (University of Ottawa, Canada), Connor Paddock (University of Ottawa, Canada), and Anne Broadbent (University of Ottawa, Canada)

Enhancing Quantum Security over Federated Learning via Post-Quantum Cryptography 499
Pingzhi Li (The University of North Carolina at Chapel Hill, USA), Tianlong Chen (The University of North Carolina at Chapel Hill, USA), and Junyu Liu (The University of Pittsburgh, USA)

Network Operations Scheduling for Distributed Quantum Computing 506
Nitish Chandra (University of Pittsburgh, USA), Eneet Kaur (Cisco Quantum Lab, USA), and Kaushik Seshadreesan (University of Pittsburgh, USA)

Entangling Intelligence: AI-Quantum Crossovers and Perspectives 516
Zhuo Chen (Massachusetts Institute of Technology, USA; The NSF AI Institute for Artificial Intelligence and Fundamental Interactions) and Di Luo (Massachusetts Institute of Technology, USA; The NSF AI Institute for Artificial Intelligence and Fundamental Interactions; University of California, USA; Harvard University, USA)

Towards Efficient and Secure Quantum-Classical Communication Networks 520
Pei Zeng (University of Chicago, USA), Debayan Bandyopadhyay (University of Chicago, USA), José A. Méndez Méndez (University of Chicago, USA), Nolan Bitner (University of Chicago, USA; Argonne National Laboratory, USA), Alexander Kolar (University of Chicago, USA), Michael T. Solomon (University of Chicago, USA; Argonne National Laboratory, USA), F. Joseph Heremans (University of Chicago, USA; Argonne National Laboratory, USA), David D. Awschalom (University of Chicago, USA; Argonne National Laboratory, USA; University of Chicago, USA), Liang Jiang (University of Chicago, USA), and Junyu Liu (University of Chicago, USA; SeQure, USA; The University of Pittsburgh, USA)

Workshop SR-CIST Agenda

Paper Session 1: CPS Security & Resiliency

Organizational Influence on Supply Chain for Digital Energy Infrastructure: Business Models, and Policy Landscape 524
Gabriel Weaver (Idaho National Laboratory, USA), Megan Culler (Idaho National Laboratory, USA), and Emma Stewart (Idaho National Laboratory, USA)

Development of a Cyber-Physical Model and Emulation of an Oil and Gas Compressor Station for Cybersecurity Research and Development 531
Adam J. Beauchaine (Sandia National Laboratories, NM), Titus A. Gray (Sandia National Laboratories, NM), Andrew S. Hahn (Sandia National Laboratories, NM), Lee T. Maccarone (Sandia National Laboratories, NM), and Scott T. Bowman (Idaho National Laboratory, ID)

On the Application of Cyber-Informed Engineering (CIE) 537
Benjamin Lampe (Idaho National Laboratory)

Formal Verification of a Nuclear Plant Thermal Dispatch Operation Using System Decomposition 543
Abhimanyu Kapuria (University of Pittsburgh, USA) and Daniel Cole (University of Pittsburgh, USA)

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

Statistical Methods for Developing Cybersecurity Response Thresholds for Operational Technology Systems Using Historical Data 549
J. Connor Grady (Sandia National Laboratories, NM), Shaw X. Wen (Idaho National Laboratory, ID), Lee T. Maccarone (Sandia National Laboratories, NM), and Scott T. Bowman (Idaho National Laboratory, ID)

Defensive Priorities in Securing Space-Based Infrastructure Dependencies 555
Joseph Slowik (The MITRE Corporation, USA)

Advancing Spacecraft Security Through Anomaly Detection 560
Nathan Wiatrek (Southwest Research Institute, USA), Kisa Burnett (Southwest Research Institute, USA), Szu-Li Lin (Southwest Research Institute, USA), Samantha Liu (Southwest Research Institute, USA), and Patrick Saenz (Southwest Research Institute, USA)

Provably Secure and Optimal Inter-Satellite Link Authentication for Low Orbit Satellites 566
Kerry Anne Farrea (Deakin Cyber Research and Innovation Centre, Deakin University, Australia), Zubair Baig (Deakin Cyber Research and Innovation Centre, Deakin University, Australia), Robin Doss (Deakin Cyber Research and Innovation Centre, Deakin University, Australia), and Dongxi Liu (Data 61, CIRSO, Australia)

Author Index **573**