

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

**Pittsburgh, Pennsylvania, USA
12-14 November 2025**

IEEE Catalog Number:
ISBN:

CFP25V08-POD
979-8-3315-9692-7



Copyright © 2025, IEEE

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:	CFP25V08-POD
ISBN (Print-On-Demand):	979-8-3315-9692-7
ISBN (Online):	979-8-3315-9691-0

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

TABLE OF CONTENTS

Enabling Privacy-Preserving Model Evaluation in Federated Learning via Fully Homomorphic Encryption	1
<i>Cem Ata Baykara, Ali Burak Ünal, Mete Akgün</i>	
Quantifying Trust in Human-AI Teams: A Statistical Framework for Task-Based Calibration of AI Autonomy in Compliance Auditing	11
<i>Priya Mohan, Yugandhar Reddy Suthari, Sahil Dhir</i>	
Upgrade or Switch: Do We Need a Next-Gen Trusted Architecture for the Internet of AI Agents?	25
<i>Ramesh Raskar, Pradyumna Chari, Mahesh Lambe, Robert Lincourt, Raghu Bala, Aditi Joshi Jared James Grogan, Abhishek Singh, Ayush Chopra, Rajesh Ranjan, Shailja Gupta, Dimitris Stripelis Maria Gorskikh, Sichao Wang</i>	
HERL: Tiered Federated Learning with Adaptive Homomorphic Encryption using Reinforcement Learning	35
<i>Jiaxang Tang, Zeshan Fayyaz, Mohammad A. Salahuddin, Raouf Boutaba, Zhi-Li Zhang, Ali Anwar</i>	
PPFL-RDSN: Privacy-Preserving Federated Learning-Based Residual Dense Spatial Networks for Encrypted Lossy Image Reconstruction	45
<i>Peilin He, James Joshi</i>	
One-Shot Secure Aggregation: A Hybrid Cryptographic Protocol for Private Federated Learning in IoT	56
<i>Imraul Emmaka, Tran Viet Xuan Phuong</i>	
RBBD: A Representation-Based Framework for Edge-Case Backdoor Defense in Federated Learning	67
<i>Samir Poudel, Kritagya Upadhyay, Jiblal Upadhya</i>	
Enhancing Resilience in Industrial Control Systems: Rapid Attack Detection, Recovery, and Monotonicity Preservation Through STL-GT Online Monitoring	78
<i>Chidi Agbo, Hoda Mehrpouyan</i>	
Robust Physically Realizable Backdoor Attack	90
<i>Md Jahirul Islam, Kazi Aminul Islam</i>	
Fidelity-Optimizing Defense Mechanism Against Membership Inference Attacks	100
<i>Md Faisal Ahmed, Zhengdao Wang</i>	
NATGVD: Natural Adversarial Example Attack Towards Graph-Based Vulnerability Detection	113
<i>Avilash Rath, Weiliang Qi, Youpeng Li, Xinda Wang</i>	
Explainable But Vulnerable: Adversarial Attacks on XAI Explanation in Cybersecurity Applications	125
<i>Maraz Mia, Mir Mehedi A. Pritom</i>	
Anomaly Detection in Graphs via Topology-Aware Attention Mechanisms	135
<i>Narges Alipourjeddi, Ali Miri</i>	
It's About Time!: Exploiting Timing Variance for IoT Device-Type Fingerprinting	143
<i>Maxwel Bar-on, Alanood Alqobaisi, Bruhadeshwar Bezawada, Indrakshi Ray, Indrajit Ray</i>	
Data Access Control in Large Language Models	154
<i>Nouha Oualha, Christophe Janneteau</i>	

Clone What You Can't Steal: Black-Box LLM Replication via Logit Leakage and Distillation	164
<i>Kanchon Gharami, Hansaka Aluvihare, Shafika Showkat Moni, Berker Peköz</i>	
PRvL: Quantifying the Capabilities and Risks of Large Language Models for PII Redaction	172
<i>Leon Garza, Anantaa Kotal, Aritran Piplai, Lavanya Elluri, Prajit Kumar Das, Aman Chadha</i>	
LLMalMorph: On the Feasibility of Generating Variant Malware Using Large-Language-Models	184
<i>Md Ajwad Akil, Adrian Shuai Li, Imtiaz Karim, Arun Iyengar, Ashish Kundu, Vinny Parla, Elisa Bertino</i>	
CoDICE: Roll the DICE for Firmware Attestation	196
<i>Rakesh Podder, Jason Simental, Elmaddin Azizli, Bharadwaj Mantha, Indrajit Ray</i>	
Limitations of Watermarking AI-Generated Speech Using AudioSeal	210
<i>Shameer Faziludeen, Arun Sankar M. S., Phillip L. De Leon, Utz Roedig</i>	
Diffusion Based Face Generation via Image Editing and Image Morphing	220
<i>Liyue Fan, Joseph Roberson</i>	
EDL: Efficient Data-Oblivious Loops	226
<i>Biniyam Tiruye, Lauren Biernacki, Todd Austin</i>	
Decoding the Decoders: An Empirical Study of Reverse Engineering Questions on Stack Exchange	239
<i>Md Rakibul Islam, Md Humaun Kabir, Anwarul Islam Sifat</i>	
PQC-LEO: An Evaluation Framework for Post-Quantum Cryptographic Algorithms	250
<i>Callum Turino, William J. Buchanan, Owen Lo, Christoph Thümmler</i>	
Explainable AI in Data Poisoning Threat Models Across the CIA Triad: A Smart Grid Case Study	261
<i>Gustavo Sánchez, Ghada Elbez, Veit Hagenmeyer</i>	
A Privacy-Fidelity Tradeoff Framework in Post-Processed Machine Learning	272
<i>Md Faisal Ahmed, Zhengdao Wang</i>	
Learning from Literature: A Retraining-Free Framework for LLM Jailbreak Defense via NLP-Based Adversarial Literature Analysis	283
<i>Sheikh Samit Muhaimin, Spyridon Mastorakis</i>	
Images in Motion?: A First Look Into Video Leakage in Collaborative Deep Learning	295
<i>Md Fazle Rasul, Alanood Alqobaisi, Bruhadeshwar Bezawada, Indrakshi Ray</i>	
Privacy-Preserving AI-Enabled Decentralized Learning and Employment Records System	306
<i>Yuqiao Xu, Mina Namazi, Sahith Reddy Jalapally, Osama Zafar, Youngjin Yoo, Erman Ayday</i>	
FALCON: Federated Anomaly Learning and Collaborative Network for Secure Autonomous Vehicles	317
<i>Riadh Ben Chaabene, Darine Amayed, Fehmi Jaafar, Mohamed Cheriet</i>	
MAVUL: Multi-Agent Vulnerability Detection via Contextual Reasoning and Interactive Refinement	327
<i>Youpeng Li, Kartik Joshi, Xinda Wang, Eric Wong</i>	
Leveraging Transformer Models and eXplainable Reinforcement Learning Methods for Advanced Intrusion Detection and Response System	338
<i>Mohammad Ghasemigol, Daniel Takabi</i>	
GPS Spoofing Attacks and Pilot Responses Using a Flight Simulator Environment	347
<i>Mathilde Durieux, Kayla D. Taylor, Laxima Niure Kandel, Deepti Gupta</i>	

VulnDetective: Using LLM Agents to Analyze Common Weaknesses and Identify Smart Contract Vulnerabilities	355
<i>Thanmai Mandala, Cora Zeger, Tessa E. Andersen, Gaby G. Dagher, Jun Zhuang</i>	
XAST: Explainable AST-Transformer for Smart Contract Vulnerability Detection	365
<i>Harshith Sai Veeraiah, Syed Badruddoja, Ram Dantu</i>	
Guiding Reinforcement Learning Using Uncertainty-Aware Large Language Models	376
<i>Maryam Shoaeeinaeini, Brent Harrison</i>	
Security of Operations on Random Numbers	385
<i>Tejas Sharma, Ashish Kundu</i>	
Experiences Building Enterprise-Level Privacy-Preserving Federated Learning to Power AI for Science	395
<i>Zilinghan Li, Aditya Sinha, Yijiang Li, Kyle Chard, Kibaek Kim, Ravi Madduri</i>	
Detection of Blacktopped Counterfeit ICs Using Surface Texture Analysis	405
<i>John M. Klamut, Mai Abdelhakim, Samuel J. Dickerson, Ashish Avachat, Heng Ban, Philip Santillo</i>	
Challenges in Identifying Illicit Actors in Financial Networks	412
<i>Amro A. Aljundi, Abhijin Adiga, Philip B. K. Potter, Samarth Swarup, Anil Vullikanti, Madhav V. Marathe</i>	
A Multi-Layered Embedded Intrusion Detection Framework for Programmable Logic Controllers	422
<i>Rishabh Das, Aaron Werth, Tommy Morris</i>	
Investigating Physical Consequences of Cyber-Attacks Using a Cyber-Physical Model of a Compressor Station	430
<i>Andrew S. Hahn, Adam J. Beauchaine, Lee T. Maccarone, Titus A. Gray, Robert S. Lois</i>	
TPM-Based Continuous Remote Attestation and Integrity Verification for 5G VNFs on Kubernetes	438
<i>Al Nahian Bin Emran, Rajendra Upadhyay, Rajendra Paudyal, Lisa Donnan, Duminda Wijesekera</i>	
Resilience to Dynamic Load Attacks Under AI Demand and Hyperscale Data Centers	448
<i>Masoud Barati</i>	
Quantitative Analysis of UAV Intrusion Mitigation for Border Security in 5G with Leo Backhaul Impairments	458
<i>Rajendra Upadhyay, Al Nahian Bin Emran, Rajendra Paudyal, Lisa Donnan, Duminda Wijesekera</i>	
Route Choice Prediction Through User Behavior Analysis: Towards Robustness Assessment Under External Perturbations	467
<i>Gustavo Sánchez, Fatih Ünal, Alexandra Wins</i>	
Grid-Computer Symbiosis: Towards the Industrial Internet of Things	472
<i>Danielle McGuire</i>	
Space-Based Fog Computing Across LEO and MEO Constellations for On-Orbit Hypersonic Detection and Space Domain Awareness	482
<i>Jackson Artis, Gregory Falco</i>	
WaveVerif: Acoustic Side-Channel Based Verification of Robotic Workflows	492
<i>Zeynep Yasemin Erdogan, Shishir Nagaraja, Chuadhry Mujeeb Ahmed, Ryan Shah</i>	
AegisBlock: A Privacy-Preserving Medical Research Framework Using Blockchain	503
<i>Calkin Garg, Omar Rios Cruz, Tessa E. Andersen, Gaby G. Dagher, Donald Winiecki, Min Long</i>	

Exploring Membership Inference Vulnerabilities in Clinical Large Language Models	512
<i>Alexander Nemecek, Zebin Yun, Zahra Rahmani, Yaniv Harel, Vipin Chaudhary, Mahmood Sharif Erman Ayday</i>	
Convergence of Operational Technology/Industrial Control Systems/Internet of Medical Things: Internet-Exposed Medical Device Threats	520
<i>J. Malakai Bailey, William Yurcik, O. Sami Saydjari, Rodolfo da Silva Avelino, João Luisi Vieira Pedro Umbelino, Gregory Pluta</i>	
Examining The CoVCues Dataset: Supporting COVID Infodemic Research Through a Novel User Assessment Study	529
<i>Shreetika Poudel, Ankur Chattopadhyay</i>	
Evaluating Security Features in Mobile Health Apps: A Systematic Review	539
<i>Yuanyuan Cao, Yi Xu, Leming Zhou</i>	
A High-Assurance Systems Approach to Medical Device Security	546
<i>Daniel G. Cole, William W. Clark</i>	
An Unsupervised Domain Adaptation Method to Enhance Diagnostic Model Resilience on Heterogeneous Medical Imaging Data	548
<i>Zhiwei Gong, Dooman Arefan, Wendie A. Berg, Shandong Wu</i>	
Privacy at Scale in Networked Healthcare	554
<i>M. Amin Rahimian, Benjamin Panny, James B.D. Joshi</i>	
Architectural Approaches to Fault-Tolerant Distributed Quantum Computing and Their Entanglement Overheads	564
<i>Nitish Kumar Chandra, Eneet Kaur, Kaushik P. Seshadreesan</i>	
Not All Qubits are Utilized Equally	576
<i>Jeremie Pope, Swaroop Ghosh</i>	
Quantum Heuristics for Linear Optimization Over Large Separable Operators	583
<i>Ankith Mohan, Tobias Haug, Kishor Bharti, Jamie Sikora</i>	
Towards Quantum-Driven Multimodal Machine Learning: Methods, Challenges, and Future Directions	593
<i>Debashis Das, Jaclyn Claiborne, Lexus Brinkley-Tapp, Mikel Houston, Pushpita Chatterjee, Uttam Ghosh</i>	
Quantum-Resistant Networks using Post-Quantum Cryptography	603
<i>Xin Jin, Nitish Kumar Chandra, Mohadeseh Azari, Kaushik P. Seshadreesan, Junyu Liu</i>	
Towards Symmetry-Aware Efficient Simulation of Quantum Systems and Beyond	609
<i>Min Chen, Minzhao Liu, Changhun Oh, Liang Jiang, Yuri Alexeev, Junyu Liu</i>	
A Decentralized Framework for Auditing Large Language Model Reasoning	613
<i>Morris Yu-Chao Huang, Zhen Tan, Mohan Zhang, Pingzhi Li, Zezhen Ding, Zhuo Zhang, Tianlong Chen</i>	
Perspective on AI-Empowered Design of Realistic Quantum Optical Devices	616
<i>Chaohan Cui, Kailu Zhou, Zheshen Zhang</i>	
Measuring Privacy Literacy on Generative AI: A Pilot Study of Generation Z	619
<i>Jing Hua, Wenli Wang</i>	

Detecting and Correcting Hallucinations in Paragraph-Level Text with Ensemble-Based Evaluation	626
<i>Shivangi Tripathi, Heena Rathore</i>	
Trustworthy LLM-Mediated Communication: Evaluating Information Fidelity in LLM as a Communicator (LAAC) Framework in Multiple Application Domains	635
<i>Mohammed Musthafa Rafi, Adarsh Krishnamurthy, Aditya Balu</i>	
Topic Modeling Analysis of Ethical Framework Separability in LLM-Generated Moral Justifications	643
<i>Bishal Thapa, Heena Rathore</i>	
The Mediating Role of Explainable AI on Phishing Susceptibility	653
<i>Masialeti Masialeti, Wenli Wang</i>	
Machine Learning-Based Frameworks for Malware Detection with SHAP Explainability	658
<i>Afia Darko Asante, Sumaila Iddrisu, Nadhem Ebrahim</i>	
Backdoor-Aware Adaptive Aggregation for Wireless Ad Hoc Federated Learning	668
<i>Atsuya Muramatsu, Hideya Ochiai</i>	
Certified Attribute Privacy in Gan Latent Space	676
<i>Jamil Arbas, Shadan Ghaffaripour, Ali Miri</i>	
Voice Design and Trust in Automated Vehicles: Findings and a Research Agenda	686
<i>Jiongyu Chen, Qiaoning Zhang</i>	
The Role of Perceived Social Identity in Human-AI Collaboration	695
<i>Jessica K. Barfield</i>	
Uncertainty Quantification for Deep Learning-Based Medical Imaging Classification Model Evaluation and Individualized Risk Estimation	701
<i>Jiren Li, Dooman Arefan, Shandong Wu</i>	
Multimodal Deep Fusion Architecture for Human Activity and Fall Detection in Elderly Care	708
<i>Debashis Das, Laure Bien Aime, Pushpita Chatterjee, Uttam Ghosh</i>	