

2025 22nd Annual International Conference on Privacy, Security, and Trust (PST 2025)

**Fredericton, NB, Canada
26-28 August 2025**

IEEE Catalog Number:
ISBN:

CFP2504F-POD
979-8-3315-0344-4



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:	CFP2504F-POD
ISBN (Print-On-Demand):	979-8-3315-0344-4
ISBN (Online):	979-8-3315-0343-7

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

A Static Analysis of Popular C Packages in Linux	1
<i>Jukka Ruohonen, Mubashrah Saddiqa, Krzysztof Sierszecki</i>	
Using Counterfactuals for Explainable Android Malware Detection	11
<i>Maryam Tanha, Winston Zhao, Aaron Hunter, Ashkan Jangodaz</i>	
Multilingual Phishing Email Detection Using Lightweight Federated Learning	22
<i>Dakota Staples, Hung Cao, Saqib Hakak, Paul Cook</i>	
A Generic Framework for Privacy Risk Assessment of Machine Learning Models	28
<i>Le Wang, Sonal Allana, Xiaowei Sun, Liang Xue, Xiaodong Lin, Rozita Dara, Pulei Xiong</i>	
TrollSleuth: Behavioral and Linguistic Fingerprinting of State-Sponsored Trolls	39
<i>Havva Alizadeh Noughabi, Fattane Zarrinkalam, Abbas Yazdinejad, Ali Dehghantanha</i>	
Privacy Preservation with Noise in Explainable AI	49
<i>Sonal Allana, Rozita Dara</i>	
RefPentester: A Knowledge-Informed Self-Reflective Penetration Testing Framework Based on Large Language Models	57
<i>Hanzheng Dai, Yuanliang Li, Jun Yan, Zhibo Zhang</i>	
FactCellar: An Evidence-based Dataset for Automated Fact-Checking	65
<i>Arbaaz Dharmavaram, Farrukh Bin Rashid, Saqib Hakak</i>	
An Intelligent Framework for Deceptive Review Detection Using Advanced Trust Vector Modeling	71
<i>Lily Dey, Md Shopon, Marina L Gavrilova</i>	
Context-Aware Location De-Identification Using Denoising Diffusion	77
<i>Md Shopon, Marina L Gavrilova</i>	
An Efficient and Privacy-Preserving AdaBoost Federated Learning Framework for AiP System	87
<i>Zhuliang Jia, Suprio Ray, Rongxing Lu, Mohammad Mamun</i>	
Dynamic Decentralized Social Trust for Financial Inclusion with Regulatory Compliance	93
<i>Suzana M. B. Maranhao Moreno, Alessandro Aldini, Paul-Antoine Bisgambiglia, Jean-Marc Seigneur</i>	
FragmentFool: Fragment-based Adversarial Perturbation for Graph Neural Network-based Vulnerability Detection	99
<i>Muhammad Fakhrur Rozi, Tao Ban, Seiichi Ozawa, Hiroaki Inoue, Takeshi Takahashi, Sajjad Dadkhah</i>	
CHOO-PIR: Hint-Based Private Information Retrieval with Commodity Servers	105
<i>Kittiphop Phalakarn, Ryuya Hayashi</i>	
Toward a Lexicon for Privacy, Security, and Trust: Analysing Digital Identity in Media using NLP	115
<i>Matthew Comb, Andrew Martin</i>	
Per-Attribute Privacy in Large Language Models Using Matrix-Variate Gaussian Mechanism	123
<i>Islam A. Monir, Gabriel Ghinita</i>	
Balancing Trade-offs: Adaptive Differential Privacy in Interpretable Machine Learning Models	133
<i>Farhin Farhad Riya, Shahinul Hoque, Yingyuan Yang, Jinyuan Sun, Olivera Kotevska</i>	

Trust-Aware Federated Defense Against Data Poisoning in ML-Driven IDS For CAVs	139
<i>Mahsa Tavasoli, Abdolhossein Sarrafzadeh, Ali Karimoddini, Milad Khaleghi, Tienake Phuapaiboon</i>	
<i>Amauri Goines, Aiden Harris, Jason Griffith</i>	
RF-RADS: A Robust Framework for Risk Assessment in Digital Substations	145
<i>Mahdi Abrishami, Kwasi Boakye-Boateng, Hossein Shokouhinejad, Emmanuel Dana Buedi</i>	
<i>Kishore Sreedharan, Shabnam Saderi Oskoue</i>	
SynQP: A Framework and Metrics for Evaluating the Quality and Privacy Risk of Synthetic Data	156
<i>Bing Hu, Yixin Li, Asma Bahamyirou, Helen Chen</i>	
Quantum Computing Threats to Management and Operational Safeguards of IEC 62351	162
<i>Brian Goncalves, Arash Mahari, Atefeh Mashatan, Reza Arani, Marthe Kassouf</i>	
Temporal-Spatial Feature Modification Attacks Against Machine Learning-Based Network Intrusion	
Detection Systems	169
<i>Sohini Pillay, Eeshan Walia, Christopher Yoeurng, Dongfeng Fang, Shengjie Xu</i>	
Cyber Threat Mitigation with Knowledge-Infused Reinforcement Learning and LLM-Guided Policies	175
<i>Md. Shamim Towhid, Shahrear Iqbal, Euclides Carlos Pinto Neto, Nashid Shahriar, Scott Buffett</i>	
<i>Madeena Sultana, Adrian Taylor</i>	
Clustering Algorithms for Anomaly Detection in EVCS Infrastructure using OCPP	185
<i>Chris Tchimmegne Tchasse, Yendoubé Kombate, Pierre-Martin Tardif</i>	
Houdini: Benchmarking Container Security Confinement	191
<i>Huzaiifa Patel, David Barrera, Anil Somayaji</i>	
On Feature Selection for Botnet Detection using Adaptive Exploration in Binary Particle Swarm	
Optimization Algorithm	201
<i>Syed Tehjeebuzzaman, Mustafa Siam-Ur-Rafique, Ashikur Rahman, Abderrahmane Leshob, Raqeebir Rab</i>	
A Dynamic, Context-Aware Trust Model for Distributed Computing Environments	211
<i>Divya Bansal, Sabrina Dhalla, Jaspal Kaur Saini</i>	
G-STAR: A Threat Modeling Framework for General-Purpose AI Systems	219
<i>Pulei Xiong, Saeedeh Lohrasbi, Prini Kotian, Scott Buffett</i>	
A Machine Learning-Based Framework for Assessing Cryptographic Indistinguishability of	
Lightweight Block Ciphers	231
<i>Jimmy Dani, Kalyan Nakka, Nitesh Saxena</i>	
DNS Profiler: Quantifying User Browsing Risk from DNS Traffic Patterns	241
<i>Mahdi Daghmehchi Firoozjaei, Yaer Baseri, Qing Tan</i>	
Encryption Struggles Persist: When Tech-Savvy Students Face Challenges with PGP in Thunderbird	247
<i>Md Imanul Huq, Ahmed Tanvir Mahdad, Nitesh Saxena</i>	
From Birthday Cheers to Privacy Fears: Unraveling the Paradox of Social Media Celebrations in	
Nigeria	257
<i>Victor Yisa, Rita Orji</i>	
Legal Retrieval Augmented Generation with Structured Retrieval and Iterative Refinement	269
<i>Chaitanya Dhananjay Jadhav, Chang Liu, Jun Zhao</i>	

Beyond SSO: Mobile Money Authentication for Inclusive e-Government in Sub-Saharan Africa	278
<i>Oluwole Adewusi, Wallace S. Msagusa, Jean Pierre Imanirumva, Okemawo Obadofin, Jema D. Ndibwile</i>	
Private Function Evaluation using CKKS-based Homomorphic Encrypted LookUp Tables	289
<i>Haoyun Zhu, Takuya Suzuki, Hayato Yamana</i>	
A Modeling and Static Analysis Approach for the Verification of Privacy and Safety Properties in Kotlin Android Apps	299
<i>Bara' Nazzal, Manar H. Alalfi, James R. Cordy</i>	
No Safety in Numbers: Traffic Analysis of Sealed-Sender Groups in Signal	305
<i>Eric Brigham, Nicholas Hopper</i>	
TOM-Net: Few-Shot IoT Malware Classification Via Open-Set Aware Transductive Meta-Learning	315
<i>Man-Ying Chen, Tao Ban, Shin-Ming Cheng, Takeshi Takahashi</i>	
Evaluating Efficient Patch-Based Backdoor Attacks in Satellite Image Classification Systems	326
<i>Ghazal Rahmanian, Pooria Madani</i>	
Exploring the Impact of Feature Selection on Non-Stationary Intrusion Detection Models in IoT Networks	336
<i>Muaan Ur Rehman, Hayretin Bahşi, Rajesh Kalakoti</i>	
Analysis of User-Generated Content to Unfold Privacy Concerns with CBDCs	346
<i>Arshpreet Singh, Mohamad Sadegh Sangari, Atefeh Mashatan</i>	
Empirical Evaluation and Reclassification of Cryptographic Algorithms for Energy-Efficient Secure Communication in Medical IoT Devices	356
<i>Sidra Anwar, Jonathan Anderson</i>	
Comparing Client- & Server-Side AEAD Encryption in Software-Defined Storage Systems	368
<i>David Mohren, Minh Truong, Brett Kelly, Kenneth B. Kent</i>	
DEDALUS & ICARUS: Image Privacy Classification Systems with Risk Oriented Explanations	375
<i>Hugo Rocha De Alba, Esma Aïmeur, Mohamed Loutis, Khulud Alqahtani</i>	
Piecewise Linear Activations for Efficient and Secure Neural Networks with GPU Acceleration	386
<i>Hiba Guerrouache, Menatallah Fadoua Slama, Yacine Challal, Karima Benatchba</i>	
Probing AlphaFold's Input Attack Surface via Red-Teaming	395
<i>Tia Pope, Ahmad Patooghy</i>	
Semantic and Graph-Based Unsupervised Learning for Insider Threat Detection Using User Activity Sequences	405
<i>Neda Baghalizadeh-Moghadam, Christopher Neal, Sara Imene Boucetta, Frédéric Cuppens</i> <i>Nora Boulahia-Cuppens</i>	
Detecting Ransomware Before It Bites: A Hybrid Model Approach for Early Ransomware Detection	412
<i>Sk Mahtab Uddin, Saqib Hakak, Miguel Garzón</i>	
LAID: Lightweight AI-Generated Image Detection in Spatial and Spectral Domains	418
<i>Nicholas Chivaran, Jianbing Ni</i>	
Short Training Techniques to Enhance Usability of System-Assigned PINs	428
<i>Israt Jahan Jui, Amirali Salehi-Abari, Julie Thorpe</i>	

Stateless Decentralized Authentication Using Segmented ZKPs for Microservices Architectures	438
<i>Vinh Quach, Ram Dantu, Sirisha Talapuru, Apurba Pokharel, Shakila Zaman</i>	
A Per-Bag Suspicion-Based Bagging Strategy for Fighting Poisoning Attacks in Classification	449
<i>Aghoghomena Akasukpe, Tomi Adeyemi, Pooria Madani, Li Yang, Miguel Vargas Martin</i>	
An Integer Programming Framework for ReBAC Policy Mining and Optimized Conformance Testing	459
<i>Padmavathi Iyer</i>	
Comparing Macro and Micro Approaches for Detecting Phishing Where It Spreads	471
<i>Mina Erfan, Paula Branco, Guy-Vincent Jourdan</i>	
Harnessing Language Models to Analyze Android App Permission Fidelity	481
<i>Yunik Tamrakar, Ritwik Banerjee, Ethan Myers, Lorenzo De Carli, Indrakshi Ray</i>	
Characterizing Event-themed Malicious Web Campaigns: A Case Study on War-themed Websites	487
<i>Maraz Mia, Mir Mehedi A. Pritom, Tariqul Islam, Shouhuai Xu</i>	
Verify All: Establish Bidirectional and Provable Trustworthiness in Microservices Architecture	499
<i>Vinh Quach, Ram Dantu, Sirisha Talapuru, Indravadan Patel, Alexis Blackwell</i>	
A Longitudinal Look at GDPR Compliance	510
<i>Brian Kim, Yang Trista Cao, K. Suzanne Barber</i>	
Detecting Deepfakes using Temporal Consistency of Facial Expression Transitions	517
<i>Renjith Eettickal Chacko, Garima Bajwa</i>	
Secret Sharing in 5G-MEC: Applicability for joint Security and Dependability	524
<i>Thilina Pathirana, Ruxandra F. Olimid</i>	
Securing Multi-Domain Systems: Intelligent ABAC Policy Learning for Cross-Domain Access Control	534
<i>Asmita Biswas, Barsha Mitra, Iqbal Gondal, Qiang Fu</i>	
TFVDFuzzer: Transformer-based Fuzzing Framework for Vulnerability Detection in Modbus Protocol	542
<i>Ahmed Reda Aldysty, Nour Moustafa, Erandi Lakshika</i>	
Cross-Boundary Privacy-Preserving Image Learning	552
<i>Atsuko Miyaji, Tomoshi Yagishita, Yuki Hyohdoh, Pierre Boudvillain</i>	
Enhancing Visual Speaker Authentication using Dynamic Lip Movement and Meta-Learning	562
<i>Pooja Pathare, Garima Bajwa</i>	
Database Systems Examination and Digital Forensics Tool: The Progress and Limitations	571
<i>Oluwasola Mary Adedayo</i>	
Assessing Privacy Practices on Ontario Municipal Websites	581
<i>Adegboola David Adelabu, Yan Yan, Wenjing Zhang, Sampsa Rauti, Ville Leppänen, Zuhaibuddin Bhutto Wenjun Lin</i>	
Identifying and Addressing User-level Security Concerns in Smart Homes Using “Smaller” LLMs	587
<i>Hafijul Hoque Chowdhury, Riad Ahmed Anonto, Sourov Jajodia, Suryadipta Majumdar Md. Shohrab Hossain</i>	
Formal Specification and Verification of Protection in Transit (PIT) Protocol Using UPPAAL	597
<i>Takwa Rhaimi, Hamed Aghayarzadeh, Rakesh Podder, Indrakshi Ray</i>	

Securing Android Inter-Process Communication (IPC) Using NGAC	603
<i>Jason Simental, Elmaddin Azizli, Mahmoud Abdelgawad, Indrakshi Ray</i>	