

2023 20th Annual International Conference on Privacy, Security and Trust (PST 2023)

**Copenhagen, Denmark
21-23 August 2023**



IEEE Catalog Number: CFP2304F-POD
ISBN: 979-8-3503-1388-8

**Copyright © 2023 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:	CFP2304F-POD
ISBN (Print-On-Demand):	979-8-3503-1388-8
ISBN (Online):	979-8-3503-1387-1
ISSN:	2574-139X

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

Table of Contents

Black-Box Attribute Inference Protection With Adversarial Reprogramming	1
<i>Hossein Abedi Khorasgani, Yang Wang and Noman Mohammed</i>	
A Rule-Language Tailored for Financial Inclusion and KYC/AML Compliance	11
<i>Alessandro Aldini, Suzana Moreno and Jean-Marc Seigneur</i>	
Saudi Arabian Perspective of Security, Privacy, and Attitude of Using Facial Recognition Technology	21
<i>Amani Alqarni, Daniel Timko and Muhammad Lutfor Rahman</i>	
Geodemographic Profiling of Malicious IP Addresses	33
<i>Nuray Baltaci Akhuseyinoglu and Usman Anjum</i>	
User modelling for privacy-aware self-disclosure	44
<i>Rim Ben Salem, Esmâ Aïmeur and Hicham Hage</i>	
Unsupervised User-Based Insider Threat Detection Using Bayesian Gaussian Mixture Models	52
<i>Simon Bertrand, Josée Desharnais and Nadia Tawbi</i>	
A TCP-based Covert Channel with Integrity Check and Retransmission	62
<i>Stefano Bistarelli, Andrea Imparato and Francesco Santini</i>	
Securing Substations with Trust, Risk Posture, and Multi-Agent Systems: A Comprehensive Approach	69
<i>Kwasi Boakye-Boateng, Ali A. Ghorbani and Arash Habibi Lashkari</i>	
Effectiveness and Information Quality Perception of an AI Model Card: A Study Among Non-Experts	81
<i>Vanessa Bracamonte, Sebastian Pape, Sascha Löbner and Frederic Tronnier</i>	
Security and Privacy Perceptions of Mental Health Chatbots	88
<i>Paulina Chametka, Sana Maqsood and Sonia Chiasson</i>	
Investigating Neural-based Function Name Reassignment from the Perspective of Binary Code Representation	95
<i>Guoqiang Chen, Han Gao, Jie Zhang, Yanru He, Shaoyin Cheng and Weiming Zhang</i>	
A Trust-Based Approach for Data Sharing in the MQTT Environment	106
<i>Liang Chen, Stilianos Vidalis and Su Yang</i>	
Efficient Three-party Boolean-to-Arithmetic Share Conversion	111
<i>Nan Cheng, Feng Zhang and Aikaterini Mitrokotsa</i>	
Attention in Differential Cryptanalysis on Lightweight Block Cipher SPECK	117
<i>Haoran Deng, Xianghui Cao and Yu Cheng</i>	
Private set intersection using RSA subgroups with constant-size encryptions	126
<i>Sigurd Eskeland</i>	

Exploration of Various Machine Learning Techniques for Identifying and Mitigating DDoS Attacks.....	133
<i>Olufunsho Falowo, Sylvia Azumah, Izunna Okpala, Emmanuel Kojo Gyamfi and Chengcheng Li</i>	
Private UAV-Assisted IoT Data Collection: An Energy-Privacy Trade-off.....	140
<i>Benjamin Fenelon, Saeede Enayati and Hossein Pishro-Nik</i>	
Combining homomorphic encryption and differential privacy in federated learning	145
<i>Arnaud Grivet Sébert, Marina Checric, Oana Stan, Renaud Sirdey and Cédric Gouy-Pailler</i>	
EL-GRILLO: Leaking Data Ultrasonically from Air-Gapped PCs via the Tiny Motherboard Buzzer	152
<i>Mordechai Guri</i>	
Improving Malicious PDF Detection with a Robust Stacking Ensemble Approach.....	163
<i>Ahmed Haj Abdel Khaleq and Miguel Garzón</i>	
PET-Exchange: A Privacy Enhanced Trading Exchange using Homomorphic Encryption .	168
<i>David Hasselquist, Jacob Wahlman and Niklas Carlsson</i>	
An Efficient Local Differential Privacy Scheme Using Bayesian Ridge Regression.....	180
<i>Andres Hernandez-Matamoros and Hiroaki Kikuchi</i>	
An Instance-based Transfer Learning Approach, Applied to Intrusion Detection.....	187
<i>Sonia Kawish, Habib Louafi and Yiyu Yao</i>	
Love or Hate? Share or Split? Privacy-Preserving Training Using Split Learning and Homomorphic Encryption	194
<i>Tanveer Khan, Khoa Nguyen, Antonis Michalas and Alexandros Bakas</i>	
UCreDiSSiT: User Credibility Measurement incorporating Domain interest, Semantics in Social interactions, and Temporal factor	201
<i>Rashid Hussain Khokhar, Sajjad Dadkhah, Tianhao Zhao, Xichen Zhang and Ali Ghorbani</i>	
DDoS Attack Dataset (CICEV2023) against EV Authentication in Charging Infrastructure.....	212
<i>Yoonjib Kim, Saqib Hakak and Ali Ghorbani</i>	
Extended km-Anonymity for Randomization Applied to Binary Data.....	221
<i>Masaya Kobayashi, Atsushi Fujioka and Koji Chida</i>	
Course-Correct to DeFi Lacking Default Deficiency.....	228
<i>David Kravitz and Mollie Halverson</i>	
RAPTOR: Advanced Persistent Threat Detection in Industrial IoT via Attack Stage Correlation	240
<i>Ayush Kumar and Vrizlynn Thing</i>	
Efficient Homomorphic Convolution for Secure Deep Learning Inference	252
<i>Xiaoyuan Liu, Hongwei Li, Xinyuan Qian and Hao Ren</i>	
A Secure Distributed Learning Framework Using Homomorphic Encryption	258
<i>Stephen Ly, Yuan Cheng, Haiquan Chen and Ted Krovetz</i>	

Systematizing the State of Knowledge in Detecting Privacy Sensitive Information in Unstructured Texts using Machine Learning.....	267
<i>Sascha Löbner, Welderufael Berhane Tesfay, Vanessa Bracamonte and Toru Nakamura</i>	
Layered Security Analysis for Container Images: Expanding Lightweight Pre-Deployment Scanning.....	274
<i>Shafayat Hossain Majumder, Sourov Jajodia, Suryadipta Majumdar and Md. Shohrab Hossain</i>	
Risk Oriented Resource Allocation in Robotic Swarm.....	284
<i>Yakov Mallah, Yuval Elovici and Asaf Shabtai</i>	
Unmasking the Dominant Threat of Data Manipulation Attack on Implantable Cardioverter Defibrillators.....	291
<i>Anisha Mitra and Dipanwita Roy Chowdhury</i>	
Re-visited Privacy-preserving Machine Learning.....	298
<i>Atsuko Miyaji, Tatsuhiro Yamatsuki, Bingchang He, Shintaro Yamashita and Tomoaki Mimoto</i>	
Verifiable and Privacy-Preserving Ad Exchange for Smart Targeted Advertising.....	308
<i>Brennan Mosher, Xiangman Li, Yuanyuan He and Jianbing Ni</i>	
AMF: Efficient Browser Interprocess Communication Fuzzing.....	317
<i>Gaoning Pan, Tianxiang Luo, Yiming Tao, Xiao Lei, Shuangxi Chen, Hui Lui and Chunming Wu</i>	
Protection against Ransomware in Industrial Control Systems through Decentralization using Blockchain.....	323
<i>Alireza Parvizimosaed, Daniel Amyot, John Mylopoulos and Hamid Azad</i>	
Privacy-Preserving Reputation System Against Dishonest Queries.....	328
<i>Kittiphop Phalakarn, Toru Nakamura and Takamasa Isohara</i>	
Securing Supply Chain: A Comprehensive Blockchain-based Framework and Risk Assessment.....	337
<i>Leila Rashidi, Windhya Hansinie Rankothge, Hesamodin Mohammadian, Rashid Hussain Khokhar, Brian Frei, Shawn Ellis, Lago Freitas and Ali Akbar Ghorbani</i>	
Write Blocker for Internet of Things Flash Technologies.....	347
<i>Matthew Roffel and Xiaodong Lin</i>	
Tapping into Privacy: A Study of User Preferences and Concerns on Trigger-Action Platforms.....	357
<i>Piero Romare, Victor Morel, Farzaneh Karegar and Simone Fischer-Hübner</i>	
Securing Multi-Environment Networks using Versatile Synthetic Data Augmentation Technique and Machine Learning Algorithms.....	369
<i>Furqan Rustam, Wajdi Aljedaani, Imran Ashraf and Anca Delia Jurcut</i>	
ThreatLand: Extracting Intelligence from Audit Logs via NLP methods.....	379
<i>Vinay Sachidananda, Rajendra Patil, Hongyi Peng, Yang Liu and Kwok-Yan Lam</i>	

An Efficient Federated Learning Framework for Privacy-Preserving Data Aggregation in IoT	385
<i>Rongquan Shi, Lifei Wei and Lei Zhang</i>	
Selective EEG Signal Anonymization using Multi-Objective Autoencoders	392
<i>Girijesh Singh, Palak Patel, Muhammad Asaduzzaman and Garima Bajwa</i>	
A Comparison of Machine Learning Algorithms for Multilingual Phishing Detection	399
<i>Dakota Staples, Saqib Hakak and Paul Cook</i>	
Transparency in App Analytics: Analyzing the Collection of User Interaction Data	405
<i>Feiyang Tang and Bjarte M. Østvold</i>	
VPASS: Voice Privacy Assistant System for Monitoring In-home Voice Commands	415
<i>Bang Tran, Sai Harshavardhan Reddy Kona, Xiaohui Liang, Gabriel Ghinita, Caroline Summerour and John Batsis</i>	
Analysis and Comparison of Deepfakes Detection Methods for Cross-Library Generalisation	425
<i>Changjin Wang, Hamid Sharifzadeh, Soheil Varastehpour and Iman Ardekani</i>	
GhostBuy: An All-Steps Anonymous Purchase Platform (ASAPP) based on Separation of Data	432
<i>Fabian Willems and Carlisle Adams</i>	
MMDSSSE: Multi-client and Multi-keyword Dynamic Searchable Symmetric Encryption for Cloud Storage	444
<i>Panyu Wu, Zhenfu Cao, Jiachen Shen, Xiaolei Dong, Yihao Yang, Jun Zhou, Liming Fang, Zhe Liu, Chunpeng Ge and Chunhua Su</i>	
Privacy-Preserving Publication of GWAS Statistics using Smooth Sensitivity	455
<i>Akito Yamamoto and Tetsuo Shibuya</i>	
MDPPC: Efficient Scalable Multiparty Delegated PSI and PSI Cardinality	467
<i>Yihao Yang, Xiaolei Dong, Jiachen Shen, Zhenfu Cao, Yunbo Yang, Jun Zhou, Liming Fang, Zhe Liu, Chunpeng Ge, Chunhua Su and Zongyang Hou</i>	
Forward-Secure Customizable Data Sharing in Blockchain-based EHR Systems	474
<i>Yanzi Yi, Xiaowen Feng, Xin Tian, Zan Peng, Yilin Liu, Hua Deng and Yujue Wang</i>	
Building Trust in Deep Learning Models via a Self-Interpretable Visual Architecture	486
<i>Weimin Zhao, Qusay Mahmoud and Sanaa Alwidian</i>	