

2025 IEEE Conference on Communications and Network Security (CNS 2025)

**Avignon, France
8-11 September 2025**



**IEEE Catalog Number: CFP25CNM-POD
ISBN: 979-8-3315-3857-6**

**Copyright © 2025 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:	CFP25CNM-POD
ISBN (Print-On-Demand):	979-8-3315-3857-6
ISBN (Online):	979-8-3315-3856-9
ISSN:	2474-025X

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

Dynamic Trust Scoring for Zero Trust at the Edge: A Multi-Factor, Context-Aware Approach.....	1
<i>Shengjie Xu, Yi Qian</i>	
Gender and Intersectional Bias in Cybersecurity for Next Generation Wireless Networks	7
<i>Sonay Caner-Yildirim, Isabella Corradini, Vesna Dimitrova, Valeria Loscri, Miranda Harizaj</i>	
Optimizing the Selection of Vulnerability Remediation Actions in Operational Technology Environments.....	13
<i>Kylie McClanahan, Marie Louise Uwibambe, Qinghua Li</i>	
Reconfiguration of Firewall Filter Rules as a Response to Industrial Control System Intrusion	19
<i>Jolahn Vaudey, Stéphane Mocanu, Gwenaël Delaval, Eric Rutten</i>	
MulShare: A Multi-Receiver Encrypted Search Scheme to Secure Cloud-Assisted EMRs Sharing.....	25
<i>Shiyuan Xu, Xue Chen, Yan Zhao, Shang Gao, Jing Wang, Siu-Ming Yiu</i>	
Next-Generation Deep Learning Integrated Drone Security: A 6G-Powered Enabled Edge Cloud Architecture	34
<i>Jia Wang, Ruitao Cheng, Abdullah Lakhani</i>	
Energy-Aware Smart Routing for Biomedical Waste Management Via Secure Edge Intelligence in 6G-Enabled CPS.....	40
<i>Yasaman Vaziri, Ali Hassan Sodhro</i>	
Shifting Signatures: The Ephemeral Nature of the Radio Fingerprint on the USRP X310	45
<i>Muhammad Irfan, Gabriele Oligeri, Savio Sciancalepore</i>	
Enabling Hybrid Edge-Level Threat Detection in O-RAN Private Networks for Resilience Enhancement	51
<i>Tsung-Yen Hsieh, Po-Hung Chen, Cheng-Feng Hung, Shin-Ming Cheng</i>	
ICS-SimLab: A Containerized Approach for Simulating Industrial Control Systems for Cyber Security Research	57
<i>Jaxson Brown, Duc-Son Pham, Sie-Teng Soh, Foad Motalebi, Sivaraman Eswaran, Mahathir Almashor</i>	
PROCATCH: Detecting Execution-Based Anomalies in Single-Instance Microservices	63
<i>Asbat Ei Khairi, Andreas Peter, Andrea Continella</i>	
Cybersecurity Awareness and Education for Young Internet Users: A Comprehensive Analysis of Prevention Strategies	72
<i>Dolantina Hyka, Jurgen Meçaj, Festim Kodra, Marija Milošević, Vladimir Ciric</i>	
Dark Drones: Can They Be Automatically Detected and Mitigated?	77
<i>Isaiah Henry-Simpson, Hortencia Mendoza, Anjie Shen, Xuecheng Wang, Yinzhi Cao, Lanier Watkins</i>	
Explainable AI in Tabular Medical Data: A Path to Trustworthy Healthcare Decisions.....	83
<i>Maham Aurang Zaib, Shams Ur Rehman, Erum Malik, Qurat-Ul-Ain Mastoi</i>	
iThelma: An Autonomous LLM Agent for Cyber Threat Hunting Via Playbook-Driven Intelligence.....	92
<i>Nick Chen, Raymund Lin, Dean Xie, Hank Lin, Sally Chen</i>	

Analyzing Sustainable Security for 6G Networks.....	98
<i>Tanesh Kumar, Zainab Alwaisi, Abhishek K. Gupta, Nitin Auluck, Petri Mähönen</i>	
Statistical Model Checking for the Analysis of Attacks in Connected Autonomous Vehicles.....	105
<i>Cinzia Bernardeschi, Adriano Fagiolini, Dario Pagani, Christian Quadri</i>	
CAPTure: Classifying APT Stages and Techniques Via Graph-Enhanced Network Flow Representations	111
<i>Md Taef Uddin Nadim, Qinghua Li</i>	
UDS Attack Taxonomy: Systematic Classification of Vehicle Diagnostic Threats	120
<i>Ali Recai Yekta, Nicolas Loza, Jens Gramm, Michael Peter Schneider, Stefan Katzenbeisser</i>	
HITL-EdgeSec: A Human-In-The-Loop Autoencoder Framework for Anomaly Detection in 6G Edge Networks	128
<i>Evangelia Konstantopoulou, Valeria Loscri, Nicolas Sklavos</i>	
XCIId: An SSI-Based Cross-Cloud Identity Wallet.....	133
<i>Mohamed Amine Ben Haj Salah, Romain Laborde, Daniele Canavese, Abdelmalek Benzekri, Mohamed Ali Kandi, Afonso Ferreira</i>	
Real-Time Risk Scoring of Ongoing Cyber Attacks.....	142
<i>Heeyun Kim, Fabian Zuluaga Zuluaga, Collins Evans, Siddhartha R Dalal, Vishal Misra, Dan Rubenstein</i>	
Applying Prompt-Based Mitigation of Gender-Role Bias in Large Language Models for Security.....	148
<i>Kyle Stein, Brandon Blackwell, Ernest Funue, Matthew Dees, Shari Watkins, Lanier Watkins</i>	
Energy-Efficient Workload Orchestration for 6G Vehicular Edge Computing.....	154
<i>Nawaz Ali, Fiza Siyal, Gianluca Aloï, Fahed Alkhabbas, Raffaele Gravina, Ali Hassan Sodhro</i>	
GNN-Based Self-Healing for Detection and Recovery of Compromised Nodes in Mission-Critical Supply Chains.....	160
<i>Uttam Ghosh, Laurent Njilla, Kristen E Oguno, Debashis Das</i>	
Applicability of LLM in Assessing the Reliability of Members to Mitigate Internal Threats.....	166
<i>Masahito Kumazaki, Hirokazu Hasegawa, Hiroki Takakura</i>	
A Federated Flower Learning-Empowered Intrusion Detection System for Vehicle 6G Fog Networks	172
<i>Pattaraporn Khuwuthyakorn, Orawit Thinnukool, Abdullah Lakhan</i>	
An Autonomic Resilient Electrical Grid for a University Campus.....	178
<i>Jam Mogavero, Rebecca Belval, Erwin Franz, Christopher Rouff, Ali Tekeoglu</i>	
Secret-Key Agreement Through Hidden Markov Modeling of Wavelet Scattering Embeddings	184
<i>Nora Basha, Bechir Hamdaoui, Attila A. Yavuz, Thang Hoang, Mehran Mozaffari Kermani</i>	
A Bayesian Trust-Based Secured Routing Protocol for Opportunistic Networks.....	193
<i>Jagdeep Singh, Sanjay K. Dhurandher, Isaac Woungang</i>	
Bluetooth Fingerprint Identification Under Domain Shift Through Transient Phase Derivative	199
<i>Haytham Albousayri, Bechir Hamdaoui, Weng-Keen Wong, Nora Basha</i>	
Explainable AI-Driven Threat Detection and Response for Industrial IoT	208
<i>Shokooh Khandan, Deniz Beyazgul, Olamide Jogunola, Yakubu Tsado, Tooska Dargahi</i>	

A Minimal Overlay-Based Framework for Transitioning Legacy Infrastructure to Zero Trust.....	214
<i>Wenjia Wang, Seyed Masoud Sadjadi, Naphtali Rishe, Arpan Mahara</i>	
A Strategic Roadmap for Phased Zero Trust Architecture Implementation in Organizations	220
<i>Adrian Rosén, Gurjot Singh Gaba, Andrei Gurtov</i>	
A Physical Layer Chaotic Encryption Method for a Wireless OFDM System	226
<i>Helena Celestino Maia, Calum Brown, John Dooley</i>	
Guardians of Privacy: Leveraging LLMs in Assistive Robotic Systems for Healthcare	232
<i>Kavyan Zoughalian, Muhammad Aitsam, Jims Marchang, Alessandro Di Nuovo</i>	
Echo: On the Limitations of Noise-Based Radio Fingerprinting Obfuscation	238
<i>Omar Adel Ibrahim, Roberto Di Pietro</i>	
An Effective and Robust Similarity-Based Phishing Website Detector in Cyber-Physical Systems.....	247
<i>Hui Chi Sit, Aysan Esmradi, Daniel W. K. Yip, Peng Sun</i>	
Analysis of QoS Degradation Attacks in Multi-Slice Containerized 5G Core Networks.....	253
<i>Jihyeon Song, Kyungmin Park, Cheolhee Park, Ikkyun Kim</i>	
Collusion-Driven Impersonation Attack on Channel-Resistant RF Fingerprinting	259
<i>Zhou Xu, Guyue Li, Zhe Peng, Aiqun Hu</i>	
Hardware Trojan Detection with Machine Learning and Power Side-Channels: A Post-Deployment Analysis	268
<i>Ashwin Koshy John, Sai Tarrun Pitta, Jaya Dofe, Jai Gopal Pandey</i>	
Performance Evaluation of 5G Roaming Security Based on PRINS.....	274
<i>Oliver Zeidler, Daniel Fraunholz, Julian Sturm, Hartmut König, Wolfgang Kellerer</i>	
Sec5GLoc: Securing 5G Indoor Localization Via Adversary-Resilient Deep Learning Architecture	284
<i>Ildi Alla, Valeria Loscri</i>	
Verifiable Alerts for 4G/5G Public Warning System	293
<i>Sourav Purification, Sang-Yoon Chang</i>	
Post-Quantum Secure Lattice-Based 5G-AKA Protocol Resistant to Malicious Serving Networks with Perfect Forward Secrecy.....	302
<i>Awaneesh Kumar Yadav, Eshika Choudhary, Onkar Garg, Madhusanka Liyanage</i>	
Closing the Visibility Gap: A Monitoring Framework for Verifiable Open RAN Operations	311
<i>Hexuan Yu, Mohaimin Al Barat, Yang Xiao, Y. Thomas Hou, Wenjing Lou</i>	
Securing xApps in Open RAN: A Hierarchical Approach to Authentication and Authorisation	320
<i>Pramitha Fernando, Pawani Porambage, Madhusanka Liyanage, Kris Steenhaut, An Braeken</i>	
ARGOS: Anomaly Recognition and Guarding Through O-RAN Sensing	329
<i>Stavros Dimou, Guevara Noubir</i>	
Dual-Branch Transformer for Anomaly-Based Intrusion Detection from Multivariate KPIs in the 5G User Plane.....	340
<i>Zixu Tian, Rishika Varma Kalidindi, Mohan Gurusamy</i>	
UAVIDS-2025: A Benchmark Dataset for Intrusion Detection in UAV Networks Using Machine Learning Techniques.....	349
<i>Qingli Zeng, Abdalrahman Bashir, Farid Nait-Abdesselam</i>	

Real-Time Detection of Multi-Stage Attacks Using Kill Chain State Machines	358
<i>Liliana Kistenmacher, Anum Talpur, Mathias Fischer</i>	
Tagging Alerts to Adversaries: ML-Enabled Classification Using MITRE ATT&CK	367
<i>Anum Talpur, Jannik Schröder, Liliana Kistenmacher, Georg Becker, Wolfram Wingerath, Mathias Fischer</i>	
RanDeceiver: Real-Time Identification and Deterrence of Ransomware Attacks	376
<i>Md Sajidul Islam Sajid, Jinpeng Wei, Ehab Al-Shaer</i>	
MetaHeart: Spoofing Vibrational Biometrics Via Dynamic Metasurfaces	385
<i>Dora Zivanovic, Jy-Chin Liao, Zhambyl Shaikhanov, Hou-Tong Chen, Chun-Chieh Chang, Sadhvikas Addamane, Daniel M. Mittleman, Edward W. Knightly</i>	
Impact of Acoustic Injection Attacks on Micro-UAVs	394
<i>Jorrit J. Olthuis, Bas Arendsen, Savio Sciancalepore, Nicola Zannone</i>	
A Trust-Aware POMDP Framework for Thwarting Data Falsification Attacks in Cooperative Driving	405
<i>Ziqi Xu, Jingcheng Li, Loukas Lazos, Ming Li</i>	
Operational Impact-Driven Cybersecurity Risk Assessment for Industrial Cyber-Physical Systems	414
<i>Bruno Paes Leao, Jagannadh Vempati, Gaurav Kumar Srivastava, Siddharth Bhela, Jesse Keller, Priyanjan Sharma</i>	
Embedding Covert Signals in Federated Learning: IEEE CNS 25 Poster	423
<i>Sang Wu Kim, Chenyu Xu</i>	
Logic, Belief Propagation and Misinformation	425
<i>Aaron Hunter</i>	
Optimizing Local LLM Deployment for 5G CVE Classification Avoiding External Data Exposure	427
<i>Pierpaolo Bene, Andrea Bernardini, Leonardo Sagratella, Nicolo Maunero, Marina Settembre</i>	
Intelligent Security Operation Centre Services for Critical National Infrastructures	430
<i>Alexios Lekidis, Maka Karalashvili, Leandros Maglaras, Konstantinos Karantzalos, George Spanoudakis</i>	
PlasTrack: Path-Independent Plasma-Induced Attacks on mmWave Sensing Tracking	432
<i>Zheshuo Li, Lingfeng Tao, Yidian Hu, Zhengxiong Li</i>	
Securing OFDM-Based ISAC Systems Against Sensing Attacks	441
<i>Jingcheng Li, Loukas Lazos, Ming Li</i>	
Securing Cellular Availability: The Wireless Blackhole Threat and Defense	450
<i>Sang-Yoon Chang, Sourav Purification</i>	
Practical Reflection Manipulation on mmWave-Based Physical Intrusion Detection	459
<i>Aliu Akinwale, Wentao Gao, Jiawei Li, Ang Li, Xiaojun Shang, Yanchao Zhang, Dianqi Han</i>	
Fission: Distributed Privacy-Preserving Large Language Model Inference	468
<i>Mehmet Ugurbil, Dimitris Mouris, Manuel B. Santos, José Cabrero-Holgueras, Miguel De Vega, Shubho Sengupta</i>	
Silver Linings in the Shadows: Harnessing Membership Fingerprinting for Machine Unlearning	477
<i>Nexhi Sula, Abhinav Kumar, Han Wang, Jie Hou, Reza Tourani</i>	

LAMLAD: LLM-Based Adversarial Attack Against Machine Learning for Android Malware Detection	486
<i>Tianwei Lan, Farid Nait-Abdesselam</i>	
Confundus: Mitigating Hostile Wireless Source Localization.....	495
<i>Saiqin Xu, Shuo Wang, Savio Sciancalepore, Alessandro Brighente, Mauro Conti</i>	
Split Happens: Combating Advanced Threats with Split Learning and Function Secret Sharing	505
<i>Tanveer Khan, Mindaugas Budzys, Antonis Michalas</i>	
Lightening Encrypted Convolutions: A GPU-Optimized Approach to Private Inference	514
<i>Menatallah Fadoua Slama, Hiba Guerrouache, Yacine Challal, Karima Benatchba, Riyadh Baghdadi</i>	
Enhancing Privacy Through Unlinkable Data Sharing with User-In-The-Loop Access Control	523
<i>Kevin Robert, Dominik Kaaser, Mathias Fischer</i>	
Non-Linear Polynomial Approximations of the Sigmoid for Plain and Encrypted Models	532
<i>Sudeepa Panta, Qinghua Li</i>	
Safeguarding Federated Learning-Based Road Condition Classification.....	541
<i>Sheng Liu, Panos Papadimitratos</i>	
IoT - FedMalDetect: Federated Learning Based Malware Detection for IoT Edge Devices.....	550
<i>Heetkumar Patel, Suresh Kumar Amalapuram, Saurabh Kumar, Bheemarjuna Reddy Tamma</i>	
Seeing Through the Threat: Adaptive Attention-Guided Backdoor Defense in Non-IID Federated Learning	559
<i>Xiang-Cian You, Arijit Karati</i>	
DistilGuard - Large Language Models for Poisoning Detection in Federated Learning	568
<i>Tharushi Nehara, Chanmini Kavinya Samaraweera, Oshan Nettasinghe, Ashen Nethsara, Chamara Sandeepa, Tharindu Gamage, Madhusanka Liyanage</i>	
Lightweight Biometric Authentication Mechanism Using PPG Signals for WBAN: IEEE CNS 25 Poster.....	577
<i>Ichrak Eddor Mnijli, Amal Sammoud, Guillaume Terrasson, Nicolas Huloux, Mariem Feki</i>	
Evaluating Post-Quantum Cryptography for Resource-Constrained AMI Gateways.....	579
<i>Sunwoo Lee, Woo-Hyun Choi, Hyuk Lim, Seunghyun Yoon</i>	
Causal Graph-Based Root Cause Analysis for ICS Sensor Streams.....	581
<i>Woo-Hyun Choi, Sunwoo Lee, Hyuk Lim, Seunghyun Yoon</i>	
Analysis of SRAM-Based PUFs on AMD Xilinx UltraScale+ FPGAs IEEE CNS 25 Poster.....	583
<i>Wakiya Schulz, Clemens Fritzs, Tobias Rosenkranz, Pascal Ahr, Antonio Saavedra, Lars Renkes, Christoph Lipps, Jörn Hoffmann</i>	
Dearming Android Apps at Install Time: The StegoDefender Case: IEEE CNS 25 Poster	586
<i>Andrea De Filippis, Danilo Dell'Orco, Lorenzo Valeriani, Alessio Merlo, Giuseppe Bianchi</i>	
We're eBPF'd: Exploring Adversarial Manipulation of ELF Files in eBPF-Based Programmable Network Stacks.....	588
<i>Joe Rose, Marco M. Cook, Filip Holik, Dimitrios Pezaros</i>	

Are Flow Correlation Attacks Effective on Tor? a Critical Evaluation of State-Of-The-Art Proposals	597
<i>Alessandro Brighente, Leonardo Cipelletta, Mauro Conti, Ludovico Latini</i>	
Comprehensive Post-Quantum Cryptography Performance Evaluations for QUIC Protocol	606
<i>Pedro Rigon, Honghao Fu, Weverton Cordeiro, Carol Fung</i>	
From Uptime to Remediation Speed: Advancing DNS Abuse Mitigation Metrics	615
<i>Carlos H. Gañán, Sión Lloyd, Sam Cheadle, Samaneh Tajalizadehkhoob</i>	
Adversarial Graph Perturbation for Smart Contract Vulnerability Detection.....	624
<i>Qi Han, Jiamin Deng, Shichang Huang, Yu Lit, Guyue Li, Shan Jiang, Zhe Peng</i>	
Anticipating the Evolution of APT Variants Using Generative AI and Reinforcement Learning.....	633
<i>Osama Iskandarani, Boubakr Nour, Makan Pourzandi, Mourad Debbabi, Chadi Assi</i>	
GANFUSION: GAN-Fused Synthetic Injection for Obfuscating Network Traffic Analysis	643
<i>Lalith Medury, Luke Robinson, Farah Kandah</i>	
SemPerGe: Unveiling Text-Based Adversarial Attacks on Semantic Communication	652
<i>Afia Anjum, Arkajyoti Mitra, Paul Agbaje, Md. Ahanaful Alam, Debashri Roy, Md Salik Parwez, Hebeeb Olufowobi</i>	

Author Index