2024 4th Intelligent Cybersecurity Conference (ICSC 2024)

Valencia, Spain
17-20 September 2024

IEEE

IEEE Catalog Number:	CFP24UB9-POD
ISBN:	979-8-3503-5478-2

**Copyright © 2024 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:	CFP24UB9-POD
ISBN (Print-On-Demand):	979-8-3503-5478-2
ISBN (Online):	979-8-3503-5477-5x

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

Keynote Speeches

Keynote 1: Distributed Intelligence in the Computing Continuum 1
Schahram Dustdar from Vienna University of Technology, Austria

Keynote 2: Intelligent Digital Twin (DT) for Wireless Systems 2
Mohsen Guizani from MBZUAI, UAE

Keynote 3: Intelligent Digital Twin (DT) for Wireless Systems 3
Ziyue Xu from Nvidia Flare, USA

Keynote 4: Federated Learning in the Age of Foundation Models 4
Peter Richtarik from KAUST, KSA

Keynote 5: Cyber Security and Network Systems (CyberNets) for Enabling Connected Vehicles and EV Charging 5
Nicholas Lane from University of Cambridge and Flower Labs, UK

Industrial tutorials

Tutorial 1: Federating Everything with Flower 6
Javier Fernandez-Marques from FlowerLabs, UK

Tutorial 2: Federated Learning at Full Scale with FEDn 7
Salman Toor from Uppsala University, Scaleout Systems, Sweden

ICSC2024

Poison Playground: Benchmarking State-of-the-Art Poisoning Attacks and Defenses on Vertical and Horizontal Federated Learning 8
Yusef Ahmed, Marom Sverdlov, Nirvana Miratnia

Finding Biases and Backdoors in an NVIDIA Morpheus Spam Detection Model 17
David Higley, Danielle A. Turner, and Ricardo A. Calix

Boosted-3R: Towards a novel framework for inferring ABAC policies 26
Sara Aboukadri, Aafaf Ouaddah, Abdellatif Mezrioui

Building a Data Space for the Public Security Domain using Smart Contracts 32
Roman Karl, Valentina Mazzonello, Bernardo Pacheco, Joao Silveira, Sven Schlarb, Veronika Siska, Axel Weissenfeld

Transforming Computer Security and Public Trust Through the Exploration of Fine-Tuning Large Language Models 39
Garrett Crumrine, Izzat Alsmadi, Jesus Guerrero, Yuvaraj Munian

Keystroke dynamics as challenge-response pair for attribute-based authentication using FaR Hash Token 48
Shashank Shekher Tripathi, Volker Skwarek

Empowering Scalable and Trustworthy Decentralized Computing through Meritocratic Economic Incentives 58
Akshar Patel

Hybrid Deep Learning Models with Adversarial Defense Mechanisms for Secure Beamforming Prediction 65
Ammar Kamal Abasi, Moayad Aloqaily, Mohsen Guizani

Enhancing MQTT Fault Tolerance and Resilience Against Broker Failures and DoS attacks with Decentralized Blockchain Architecture 71
Elisee Toe, Fehmi Jaafar

Brain-Computer Interface Security: Vulnerabilities of the Capsule Network Model 80
Nour El Houda Sayah Ben Aissa, Chaker Abdelaziz Kerrache, Ahmed Korichi, Abderrahmane Lakas, Enrique Hernandez Orallo, Carlos T. Calafate

Evaluating Attack Thresholds in Proof of Stake Blockchain Consensus Protocols 87

Akshar Patel

Blockchain Support for Verifiable Split Learning **95**
Carlos Beis-Penedo, Rebeca P. Diaz-Redondo, Ana Fernandez-Vilas, Francisco Troncoso-Pastoriza, Manuel Fernandez-Veiga

Category Prediction of Financial Fraud Related Posts in Telegram Group Chats **103**
Chunlan Gao, Yubao Wu

Anomaly Traffic Detection In Smart Home Using Insight From Exploratory Data Analysis **110**
Oluwasegun Apejoye, Asmau Wali, Xiaoqi Ma, Jun He, Nemitari Ajienka

Penetration testing and exploitation of Active Directory configuration vulnerabilities **118**
Zlatan Moric, Vedran Dakic, Jasmin Redzepagic, Filip Otocan

Enhancing Network Security Through Deep Learning: Mitigating Feature Engineering and Zero-Day Attacks **127**
Ibrahim EL Didi, Fouad Trad, Ali Chehab

Linking Threat Agents to Targeted Organizations: A Pipeline for Enhanced Cybersecurity Risk Metrics **132**
Spencer Massengale, Philip Huff

Enhancing OT Threat Modelling: An Effective Rule-Based Approach for Attack Graph Generation **142**
Giulio Sunder, Alberto Salvatore Colletto, Sara Raimondi, Cataldo Basile, Alessio Viticchie, Alessandro Aliberti

MitM Cyber Risk Analysis in OCPP enabled EV Charging Stations **151**
Safa Hamdare, David J.Brown, Omprakash Kaiwartya, Yue Cao, Manish Jugran

An International Framework for Cybersecurity Incident Collaboration **158**
Clariel Arias, Thaier Hayajneh

Autonomous and adaptive cyber-defense: application of game theory in 5G security architectures **166**
Wassim M.L Koribeche, David Espes, Cedric Morin

Context-Aware Security and Post Quantum Cryptography applied to IoT networks **175**
Arturo Holgado, Jorge Portilla, Daniel Lopez-Fernandez, Luis Redondo

Latent states: model-based machine learning perspectives on cyber resilience **180**
Marin Francois, Pierre-Emmanuel Arduin, Myriam Merad

Privacy Analysis in Mobile Apps and Social Networks using AI Techniques **188**
Daniel Blanco-Aza, Antonio Robles-Gomez, Rafael Pastor-Vargas, Llanos Tobarra

Accessing the Power of Machine Learning to Detect Fake News **196**
Imen Ben Ahmed, Joao Paulo Magalhaes

Web Phishing Net (WPN): A scalable machine learning approach for real-time phishing campaign detection **206**
Muhammad Fahad Zia, Sri Harish Kalidass

Generative AI for Advanced Malware Detection **214**
Mohammad Al Balawi, Mohammad Alnabhan, Mohammed S Atoum

L1TF Foreshadow CPU Vulnerabilities Analysis and Mitigation **222**
Lo’ai Tawalbeh, Harry Staley Jr., David Velez, Artem Skitenko, Abdelrahman Tawalbeh, and Fadi Muheidat

Unsupervised Insider Threat Detection Using Multi-Head Self-Attention Mechanisms **228**
Simon Bertrand, Pascal Germainy, Nadia Tawbi

Improvising Host-Based Intrusion Detection Systems by Integrating Open-Source Tools **237**
Ahmed Taha, Pabitra Kumar Roy

Detecting Free-Riders in Federated Learning using an Ensemble of Similarity Distance Metrics **245**
Sarhad Arisdakessian, Omar Abdel Wahab, Osama Wehbi, Azzam Mourad, Hadi Otrok