2025 5th Intelligent Cybersecurity Conference (ICSC 2025)

Tampa, Florida, USA
19-22 May 2025

IEEE Catalog Number: CFP25UB9-POD
ISBN: 979-8-3503-9293-7

**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:	CFP25UB9-POD
ISBN (Print-On-Demand):	979-8-3503-9293-7
ISBN (Online):	979-8-3503-9292-0

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

CURRAN ASSOCIATES INC.
proceedings.com

TABLE OF CONTENTS

Detection of Fileless Malware 1
Bhaskar Pal, G. Hitesh Reddy, Saurav S., Vasudevan A. R.

Mining Intrusion Analysis Diamonds from Security Information and Events Logs 9
Mahmoud Al-Maani, Mohammed Alsaleh

Lightweight Post-Quantum Cryptographic Solutions for IoT: A Practical Approach 17
Mohammed El-Hajj

Adaptive Cyber Attack Projection Through Context-Driven Model Selection: Combining Graph Attention Networks and Reinforcement Learning 27
Mouhamadou Lamine Diakhame, Chérif Diallo, Mohamed Mejri

Web3 Architecture's Inherent Cybersecurity Through Data and Information Safeguards 35
Collin Connors, Dilip Sarkar

DeFeAt: Explanable TinyML-Based Framework for Anomaly Detection in Nano-Sensor Traffic in 6G-Enabled Smart Grid 43
Dharma Trivedi, Shreya Bhatia, Shivanshi Bhatt, Lakshin Pathak, Krisha Shastri, Karm Vyas, Dev Mehta, Rajesh Gupta, Sudeep Tanwar

Blocking Fake News Propagation Exploiting OSNs Users Interests and Connections 49
Farwa Batool, Giuseppe Lo Re, Marco Morana, Giuseppe Rizzo

Anomaly Detection and Clustering for Resource Usage Segmentation in Cloud Data Centers 55
Mustafa Daraghmeh, Fadi Alzhouri, Anjali Agarwal, Yaser Jararweh

Blockchain for Critical Infrastructure Security: Applications and Challenges 62
Udit Gulati, Mahesh Narayanan

Privacy-Preserving Mitigation of Poisoning Attacks in Three-Tier Federated Learning 68
Ming Liu, Wensheng Zhang

AI-Driven Adaptive Gait Biometrics: Pioneering Real-Time Continuous Authentication for Enhanced Security 76
Mehdi Mekni, Emmanuel O. Ogunwobi, Shannon C. Russell, Mohamad Nassar, Adwoa Donyina

AI-Powered Threat Detection and Response: Leveraging Machine Learning for Real-Time Intrusion Detection Systems (IDS) Using Network Traffic Data 84
Mohammed El-Hajj

DeepTrAnS: Mixer-Based Unsupervised Time Series Anomaly Detection for Servers 91
Muhammad Anas Raza, Mohammad Wardat, Anyi Liu

From Abstract Prompts to Cybersecurity Labs: Automating Virtual Environment Design and Deployment with Multi-Agent Systems and LLM-Driven Orchestration 99
Yaseen Ahmed, Ali Eissa, Omar Harb, Omar Miniesy, Ziad Miniesy, Mohamed Noureldin, Amr El Mougy

Investigating UXSS Vulnerabilities in Modern Web Browsers 108
Hrishikesh Dahale

CRICE: Cyber Range Infrastructure for Cybersecurity Education 117
Sajal Bhatia, Irfan Ahmed, Nitin Talreja

BPMN Model to Smart Contract by Business Analyst 122
Christian Gang Liu, Peter Bodorik, Dawn Jutla

A Device-Centric and Temporal Learning Framework for Malicious IoT Traffic Detection 130
Mustafa Daraghmeh, Islam Obaidat, Yaser Jararweh, Anjali Agarwal, Kuljeet Kaur

Deep Learning-Driven Automated Data Generation for Enhanced Anomaly Detection in Cybersecurity 137
Michael Gough, M. Ali Akber Dewan, Harris Wang

CATCH: A Tool to Automatic Deploy Decoys and Breadcrumbs Based on Network Analysis 147
Pushpinder Kaur Chouhan, Maurizio Colombo, Rasool Asal, Zhan Cui

Securing Wireless SDN Controller from Jamming Attack 155
Chandan Kumar, Md. Sarfaraj Alam Ansari

Evaluating Privacy-Preserving Strategies in Bitcoin and Beyond 162
Chaitanya Rahalkar, Anushka Virgaonkar

Keyed Randomization with Adversarial Failure Curves and Moving Target Defense 169
Francesco Bergadano, Sandeep Gupta, Bruno Crispo

Leveraging Large Language Models for Fault Detection in Connected Vehicles 177
Rakesh Das, Henry Griffith, Heena Rathore

From Transaction to Transformation: AI and Machine Learning in FinTech 187
Yazan Al Ahmed, Abdulla Osman, Abrar Hamdi Ahmed, Dina Omar Salem, Yanal Al Ahmad

Highlight to Explain: A Case Study on Explainable AI for Pattern Discovery in Code 197
Ohamad Nassar, Jacques Bou Abdo

API Security Framework for Multi-Controller Architecture in Software-Defined Networking 206
Sumit Badotra, Mohan Gurusamy

Analysis and Evaluation of ToN IoT Windows and Garage Door Datasets 214
Yousef Sharrab, Abdel-Rahman Al-Ghuwairi, Ashraf Alomoush, Abdullah Al-Husini, Daniel Al-Burgan, Izzat Alsmadi

A Lightweight and Efficient Intrusion Detection System for Drone Networks 219
Fawaz J. Alruwaili, Cihan Tunc

Advanced Document Processing Using LLM and RAG: An Innovative Approach to Efficiency and Privacy 227
Krzysztof Kocot, Mateusz Plonka, Kacper Holda, Krzysztof Daniec, Aleksander Nawrat

LLaVul: A Multimodal LLM for Interpretable Vulnerability Reasoning About Source Code 232
Ala Jararweh, Michael Adams, Avinash Sahu, Abdullah Mueen, Afsah Anwar

Mitigating Ransomware Attacks in Internet of Medical Things Networks 242
Usman Tariq, Fehmi Jaafar, Yasir Malik

ProSoccerTrainer: A Secure AI-Powered Penalty Detection and Performance Recommendation System 248
Kushagra Nagar, Upendra Singh

Consensus-Driven Intrusion Detection Systems: Enhancing Performance and Fault-tolerance Using Approximate Consensus 256
Kritee Neupane, Lewis Tseng, Moayad Aloqaily

Tailored Large Language Models for Spam Detection: from Model Customization to Benchmarking Effectiveness 264
Amani Shatnawi, Anas Alsobeh, Izzat Alsmadi, Bilal Al-Ahmad

Reward Hacking in Reinforcement Learning and RLHF: A Multidisciplinary Examination of Vulnerabilities, Mitigation Strategies, and Alignment Challenges 272
Tiechuan Hu, Wenbo Zhu, Yuqi Yan

Relationship-Based Distributed and Variable Trust Metrics for Secure Computing 276
John M. Acken, Naresh K. Sehgal, Sonali Fernando, Divya Bansal, Robert B. Bass

Time Series Based Network Intrusion Detection Using MTF-Aided Transformer 283
Poorvi Joshi, Mohan Gurusamy

Impact of Target Network-Specific Data on the Performance of Machine-Learning-Based Intrusion Detection System Models 290
Alexander Lawall, Thomas Zöller

Revisiting Fidelity in Explainable AI: Unpacking Cognitive Biases and Deceptive Transparency in Model Interpretations 298
Akshar Patel

Privacy-Preserving Training and Inference of CNNs: A Medical Performance Case Study 303
Thomas Prantl, Louis Schneider, Simon Engel, Lukas Horn, Vanessa Borst, Christian Krupitzer, Samuel Kounev, Rafael I. Bonilla

Evolution of the Tor Network: An Empirical Analysis of Usage Patterns and Infrastructure 312
Chaitanya Rahalkar, Anushka Virgaonkar

Towards Holistic Evaluation of Intrusion Detection Systems: Insights into Latency and Detection Metrics 319
Sandhyarani Dash, John M Acken, Ruimin Dai

Neuro-Symbolic Approaches for Cybersecurity Policy Enforcement 327
Srikanta Datta Tumkur, Vinoth Ganesh Umamageswari Asokan

Rule-Based Hybrid Adaptive Encryption Model for Autonomous Flight to Secure UAS Data Streams in Real-Time 333
Fadjimata I. Anaroua, Yongxin Liu, Hong Liu

Optimizing DDoS Attack Detection in SDN Using Machine Learning 341
Rolph Abraham Yao, Ferdinand Tonguim Guinko

Quantum-Assisted XAI-Driven DL Framework for FDI Detection in Connected Autonomous Electric Vehicles Underlying 6G 349
Dev Mehta, Vrutik Soni, Param Desai, Dharma Trivedi, Lakshin Pathak, Rajesh Gupta, Sudeep Tanwar

Technology Platforms for Cybersecurity: A Comparative Analysis 355
Quispe Carlos, Reynaga Johnny, José Santisteban

Edge-Based AI for Real-Time Threat Detection in 5G-IoT Networks: A Comparative and Architectural Review 359
Alexandre Sousa, Luís Correia, Manuel J. C. S. Reis

Enhancing Error-Minimizing Noises Using Data Augmentation 364
Long Dang, Thushari Hapuarachchi, Kaiqi Xiong

AI-Enhanced Telehealth Platforms: A Comprehensive Analysis of Automated Triage and Personalized Care Systems 370
Sudheer Kumar Lagisetty, Priya Devarajulu, Anil Kumar Moka

Holistic Ethical Commons: A Dynamic Framework for Ethical Decision Making in Multi-Agent AI Systems 378
Raghavan Krishnasamy Lakshmana Perumal

Real-Time Anomaly Detection: A Hybrid Approach Combining Streaming SQL and Hardware Acceleration 385
Anil Kumar Moka, Sudheer Kumar Lagisetty

Formulation of a Contingent and Resilient Response to Cyber Security Threats Jordanian Government Digital Services 393
Razan Almomany, Mohammad Habes, Dina Tahat, Khalaf M. Tahat, Makrem Ziani

Safeguarding the Artificial Pancreas: A Review of Security and Reliability Gaps and AI Driven Resilience 399
Venkata Sai Abhinav Piratla, Sahaj Saxena, Sajal Bhatia, Navin Kumar

Enhancing IoT Attack Classification Through Domain Generalization 412
Iram Bibi, Tanir Ozcelebi, Nirvana Meratnia

Intelligent Anomaly Detection in Database Security: A Triple-Loop Learning Framework 420
William Kandolo

Author Index