

2025 Cyber Awareness and Research Symposium (CARS 2025)

**Grand Forks, North Dakota, USA
27-30 October 2025**

Pages 1-456



**IEEE Catalog Number: CFP25UW5-POD
ISBN: 979-8-3315-9629-3**

**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:	CFP25UW5-POD
ISBN (Print-On-Demand):	979-8-3315-9629-3
ISBN (Online):	979-8-3315-9628-6

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

Organizational Adoption of Post-Quantum Cryptography: Drivers, Barriers, and Strategic Implications	1
<i>Daniel Zimmermann, Peter V. Rajsingh, Elyson De La Cruz, Hermano J. De Queiroz, Shaila Rana, Geeta S. Nadella</i>	
The Unseen Impact: A Critical Investigation of Healthcare Cybersecurity Breaches using HHS Data	7
<i>Chandra Prakash, Elyson De La Cruz</i>	
Combating Cybercrime in India's Digital Age: Prediction and Prioritisation.....	14
<i>Kandaswamy Paramasivan, Sriram Ravichandran, Anusha Kumar, Nandan Sudarsanam</i>	
ETDI: Mitigating Tool Squatting and Rug Pull Attacks in Model Context Protocol (MCP) by using OAuth-Enhanced Tool Definitions and Policy-Based Access Control	23
<i>Manish Bhatt, Vineeth S. Narajala, Idan Habler</i>	
Interpreting Office Document Macros with Bi-Directional Transformer Models	29
<i>Mahesh Kalappattil, Varghese M. Vaidyan, Gurcan Comert, Yong Wang</i>	
COALESCE: Economic and Security Dynamics of Skill-Based Task Outsourcing Among Team of Autonomous LLM Agents.....	35
<i>Manish Bhatt, Ronald F. Del Rosario, Vineeth S. Narajala, Idan Habler</i>	
Security Architecture as a Service (SAaaS) for Visual Modeling and Trade-Off Analysis of Security, Availability, and Maintainability	44
<i>Ravindra K. Gautam, Prakash Ranganathan</i>	
Fast Deep Learning Voltage Security Assessment Considering Varying Network Topologies.....	52
<i>Rehan Nawaz, Santiago Grijalva</i>	
Resilient Semantic Image Delivery Under Jamming Attacks: A Comparative Study of OSTBC and OSFBC	58
<i>Shadman R. Doha, Ahmed Abdelhadi</i>	
A Deep Learning Approach to Multi-Image Steganography	65
<i>M. Rishik Srivatsal, Abbu B. Siddique, Shaik S. Rohit, V. N. N. M. Vedanth, Arunima Das, Kattamanchi Chandana, Jay Dave</i>	
Advancing File System Forensics: A Comprehensive Study of F2FS and Emerging File Systems	73
<i>Osayomore O. Aigbogun, Bing Zhou</i>	
LibLMFuzz: LLM-Augmented Fuzz Target Generation for Black-Box Libraries	80
<i>Ian Hardgrove, John D. Hastings</i>	
Dark Patterns and Consumer Protection Law for App Makers.....	86
<i>Gregory M. Dickinson</i>	
Beyond the Cable: An Experimental Study of USB Debugging Exploits on Android Devices	92
<i>Wanni V. I. Perera, Bing Zhou</i>	
Ransomware Detection using LLMs and GraphRAG	100
<i>Stefaan Bielen, Clara Maathuis, Stefano Schivo</i>	

Ground Up Approach to Zero Trust in Hybrid Environment.....	108
<i>Dipankar Saha</i>	
Blockchain-Based Authorization in UEFI Firmware for DaaS Applications	113
<i>Rui Mendonça, Maria Tavares, Paulo Maio, António Pinto</i>	
Autonomous Penetration Testing: Solving Capture-the-Flag Challenges with LLMs.....	121
<i>Isabelle Bakker, John Hastings</i>	
Modern SaaS Security Challenges and Defense Strategies	127
<i>Dipankar Saha</i>	
Empirical Analysis of Security Vulnerabilities in Open Source Software using Static Analysis Tools.....	133
<i>Donghoon Kim, Hokeun Kim</i>	
Autonomous Multi-Agent Cyber Defense: A Novel Approach using Reinforcement Learning with Hierarchical LLM Critics	141
<i>Haseeb Ahmed, Shahrear Iqbal, Euclides C. P. Neto, Scott Buffett, Madeena Sultana, Adrian Taylor</i>	
A Deep Learning Framework for Robust N-1 Power System Security Evaluation Considering Renewable Energy Generation and Topological Variation	146
<i>Adam King, Santiago Grijalva</i>	
Analyzing the Impact of Adversarial Examples on Explainable Machine Learning	155
<i>Prathyusha Devabhakthini, Suvendu Nayak, Raj Shukla, Sasmita Parida, Tapadhir Das</i>	
Privacy-Aware RAG-Enabled LLMs for Collaborative AI in Organizations	163
<i>Georgios Fragkos, Bradley Marx, Sasha Safonov, Robert Manley, Winnie Patta, Shelby Hiens</i>	
Reinforcement Learning Based Autonomous Formation for Resilient Vehicle Platoon Networks	171
<i>Istiaq Mahmud, Sherif Gaweesh, Ahmed Abdelhadi</i>	
Can Large Language Models Be Used to Conduct Attacks on Smart Home Devices?	178
<i>Jennifer D.-O. Eriagbondia, Mehdi Sookhah, Ahmad Patooghy</i>	
An Ethically Grounded LLM-Based Approach to Insider Threat Synthesis and Detection	185
<i>Haywood Gelman, John D. Hastings, David Kenley</i>	
Phishing Email Detection with Data Augmentation using LLMs.....	191
<i>Johnna Nance, R. E. Davis, Jinsheng Xu, Xiaohong Yuan, Kaushik Roy</i>	
An Advanced Deep Learning Approach for Monkeypox and Other Skin Lesion Classification.....	200
<i>Kazi S. Sharif, Mohammad N. Nayyem, Jahirul Islam, Dill M. Tabila, Touhid Imam, M. A. H. Raju</i>	
A Fast Deep Learning Framework for Real-Time Voltage Security Assessment in Power Systems	209
<i>Rehan Nawaz, Santiago Grijalva</i>	
Testbed Access Security Evaluation and Reporting (TASER) Framework: A Framework for Selecting Appropriate Access Control	215
<i>Leslie A. Viviani, Akshay R. Ramchandra, Shree R. A. Balaji, Prakash Ranganathan</i>	
Performance Study on a Kubernetes Based Learning Platform for AI Education and Workforce Training	225
<i>Wenlinag Chen, Tianzong Zhang, Sumendra Singh, Michael Tu</i>	

Evaluating the Effectiveness of Existing Phishing Detectors on AI Generated Phishing Emails.....	232
<i>Amon Ferrell, Jinsheng Xu, Hamidreza Moradi, R. E. Davis, Kaushik Roy</i>	
Optimizing a Model-Agnostic Measure of Graph Counterdeceptiveness via Reattachment.....	236
<i>Anakin Dey, Sam Ruggerio, Manav Vora, Melkior Ornik</i>	
Domain Focused Sequence Model Architecture for Predicting Long Term User Interests	243
<i>Vinay Venkatesh, Akshay Mittal, Nikita Kothari, Varun Joshi</i>	
Q-DTN: A Quantum-Enhanced Framework for Secure Financial Risk Management.....	249
<i>Akshay Mittal, Krishna Kandi, Anusha Nagineni, Vamsi Alla</i>	
File Importance Assessment Method Based on Multifaceted Proximity Propagation.....	257
<i>Yuki Kodaka, Masahito Kumazaki, Hirokazu Hasegawa, Hiroki Takakura</i>	
C/N ₀ Analysis-Based GPS Spoofing Detection with Variable Antenna Orientations.....	264
<i>Vienna Li, Justin Villa, Dan Diessner, Jayson Clifford, Laxima N. Kandel</i>	
SDR Implementation of MU-MIMO Semantic Communication Under Jamming Attacks	271
<i>Shadman R. Doha, Istiak Mahmud, Ahmed Abdelhadi</i>	
Enhancing Vehicle Safety & Security via MIMO OFDM-Based ISAC System	278
<i>Istiaq Mahmud, Sherif Gaweesh, Ahmed Abdelhadi</i>	
Enhancing Incident Response for Cloud Data Breaches: Challenges, Best Practices, and Policy Recommendations	285
<i>Ming Liu, Tianyou Liu, Zhenyu Huang</i>	
Cybersecurity Club and Team Practices: A Qualitative Multisite Study of Engagement and Success Strategies	297
<i>Johnathan Yerby, Matthew Coburn</i>	
Leveraging Internet Speed Tests as a Covert Channel for Data Exfiltration	303
<i>Janessa Palmieri, Andrew Kramer</i>	
Hybrid Fuzzing with LLM-Guided Input Mutation and Semantic Feedback.....	310
<i>Shiyin Lin</i>	
RAG-Based Code Intelligence for Real-Time Fault Diagnosis in Enterprise Systems	319
<i>Vishnupriya S. Devarajulu, M. Usha Rani, N. V. Muthu Lakshmi, L. U. K. Reddy</i>	
AI-Enabled Infrastructure Management: A Comprehensive Framework and Empirical Analysis from Platform Engineering Perspective.....	325
<i>Goutam Tadi, Akshay Mittal</i>	
Automated Detection of Identification Documents with Open Source Face Detection and Text Recognition Libraries	333
<i>Anasofia Colón-Santiago, Gianna Uyemura, José Ortiz-Ubarri</i>	
The Impact of a Targeted Scholarship Program on Cybersecurity Career Development: An Analysis Through the Lens of Social Cognitive Career Theory and Career Identity	340
<i>Portia Pusey, Faisal Kaleem, Kyle Swanson</i>	
Embedding Accountability in the AI Lifecycle for Critical Finance Applications	345
<i>Vishnupriya S. Devarajulu, Sunitha Kanipakam, Santosh R. Addula, P. Venkata Krishna</i>	

Siamese mViT: Lightweight Biometric Facial Recognition for Edge Devices.....	353
<i>Kanchon Gharami, Shafika S. Moni, Laxima N. Kandel</i>	
Balancing Privacy, Trust, and Functionality in Wearable AI: Case Studies of the Meta RayBan Glasses and PLAUD NotePin.....	361
<i>Joëlle Malacko, Ashley Podhradsky</i>	
Explaining Deep Models: A Comparative Grad-CAM CT Kidney Classification Framework	367
<i>Kazi S. Sharif, Touhid Imam, M. Minhazur Rahman, Mohammad N. Nayyem, Mohammed M. Uddin, M. Abubakkar</i>	
Military AI Security Assessment Model.....	378
<i>Clara Maathuis, Kasper Cools</i>	
Graph-Driven Unsupervised Learning for Illicit Bitcoin Transaction Detection.....	385
<i>Anand Choubey, Prakash Ranganathan</i>	
Introducing Axlerod: An LLM-Based Chatbot for Assisting Independent Insurance Agents.....	391
<i>Adam Bradley, John Hastings, Khandaker M. Ahmed</i>	
Assessing the Cybersecurity User Experience (UX) in an Organizational Context	397
<i>Shreenandan Rajarathnam, Vandana Singh</i>	
Preliminary Results: Cybersecurity Students' Attitudes Towards Hands-On Learning	406
<i>Mathew H. Van Horn, Christopher Warner</i>	
A Brief Study of Cybersecurity Penetration Testing Methods and Their Applications	409
<i>Ashkan Hosseini, Hossein Salehfar</i>	
From Bare Metal to Bare Minimum: Reframing Responsibility in Serverless Computing using LynxLab	419
<i>Nimish Sharma, Shivam Dhar</i>	
ASCTM: A Swarm Optimization-Enhanced LSTM Framework for Intelligent Intrusion Detection.....	425
<i>M. Wahidur Rahman, M. Habibur Rahman, Avdesh Mishra, Mais Nijim, Ayush Goyal, David Hicks</i>	
Towards Secure Healthcare: Intrusion Detection with GraphSAGE-Based Meta-Learning and Hybrid Deep Models	431
<i>Abel Degu, Nnaemeka Igwe, Youssef Harrath, Cole Drumheller</i>	
Power Anomaly Detection using Machine Learning for Microgrid Applications	438
<i>Adam Stowe, Richard Alves, Preetha Thulasiraman, Giovanna Oriti</i>	
A Case Study on Delegating Critical Tasks to Agentic AI and Prototype Access Control Methods.....	446
<i>Sunyoung Kim, Hokeun Kim</i>	
Behavioral Anomaly Detection in Cyber Systems via Deep Recurrent and Attention Models	451
<i>Ayhan Arisoy, Merve V. Arisoy</i>	
Constraint-Based Neural Input Optimization (NIO) for Secure Token Generation.....	457
<i>Ricardo A. Calix, Tae- Hoon Kim</i>	
Deep Isolation Forest-Based Anomaly Behavior Analysis for Internet of Medical Things.....	463
<i>Preeti Choubey, Qinxuan Shi, Zhanglong Yang, Brian Terry, Sicong Shao, Tingjun Lei</i>	

Trust and Resilience in Connected Aviation Systems.....	470
<i>Ricky Katsuya, Xiang Liu</i>	
Deconstructing Android Social Media Apps: A Static Analysis and Privacy Risk Assessment.....	478
<i>Kevin Day, Khaled Rabieh, Faisal Kaleem</i>	
Cybersecurity Education Outreach to Immigrant Communities in the U.S.: A Case Study	486
<i>Kevin Huang, Marc J. Dupuis</i>	
Bayesian Convolutional Neural Networks for Anomaly Detection in Power Systems	494
<i>John McClinton, Patrick McClure, Preetha Thulasiraman</i>	
Cybersecurity is Stressful: The Impact of Stress on Identifying Phishing Attacks.....	500
<i>Christian Bergh, Marc J. Dupuis</i>	
Classical vs. End-to-End Learning Approaches to Robot Pathfinding in Digital Twin Environments.....	508
<i>Miguel Gapud, George W. Clark, J. Todd McDonald, N. Gong</i>	
A Hybrid Deep Learning and Quantum Feature Selection Framework for Multi-Class Intrusion Detection	516
<i>Ilhan Uysal, Utku Kose</i>	
Deepfake Detection as a Service: Enabling Trust on Mobile Devices	525
<i>Abhijeet Zilpelwar, Ansh Tiwari, Raghu S. Iyengar</i>	
Synth Vuln: An Asset and Findings Generator Supporting Vulnerability Management Research	530
<i>Logan Scott, Jeremy Cohen</i>	
Hierarchical Firmware-Level Security Policy for Industrial Control Systems	538
<i>Sameer Mankotia, Daniel C. De Leon, Jennifer Johnson-Leung</i>	
Evaluating Classical and Quantum Machine Learning for Credit Card Fraud Detection: Performance and Economic Impact.....	544
<i>Muhammad Bhutta, Abid Mehmood</i>	
Attention-Enabled Fusion Based Multi Class Malware Family Classification using Large Scale BCCC-Mal-NetMem-2025 Dataset.....	553
<i>Shivani Gautam, Simone A. Ludwig</i>	
Security Framework for Agentic Home AI in Preventive Healthcare: Cyber Threats Worth Noting	559
<i>Collins P. Obeng, Nethshan M. Narasinghe, Ryan Striker, Enrique A. Vazquez</i>	
Adopting AI in Computing-Based Interdisciplinary Curricula for Workforce Readiness	564
<i>Amith K. Belman, Maryam Khazaei, Melody Moh</i>	
From Raspberry Pi to Nvidia Jetson: Boosting Cyber Awareness and Propelling Future Leaders Through Cyber-AI Summer Camps.....	572
<i>Amith K. Belman, Meien Li, Kaikai Liu, Anish Roy, Xiao Su, Melody Moh</i>	
Applying Privacy-Enhancing Technologies to LLMs in Critical Infrastructure Contexts.....	580
<i>Katherine Grillaert, Ed Vocke, Joshua Scarpino, Esther Y. Chung, Thomas Winston</i>	
Recurrent Biases and Fallacies in Dataset-Driven Intrusion Detection Research	585
<i>Mamdouh Muhammad</i>	
Fake News Detection in Bangladesh using GPT-4 with Retrieval-Augmented Generation.....	594
<i>Ernesto Rafin, Jaafar Alghazo, Wordh Ul Hasan</i>	

Securing AI Systems Through Transparency: A CIA Triad-Based Analysis	600
<i>Esther Y. Chung, Ian Hamilton, Laura Morgan, Katherine Grillaert, Joshua Scarpino</i>	
Latent Space Stochastic Perturbation Schedule via Cosine Annealing Scheduler for Privacy-Preserving Variational Autoencoders.....	606
<i>Lawrence Owusu, Ahmad Patooghy, Masud R. Rashel, Gurcan Comert, Balakrishna Gokaraju, Islam A. Kamrul</i>	
An eBPF-Based Scheduler for the AFL++ Fuzzer	613
<i>Ernesto Ortiz, Clemente Izurieta, Ann M. Reinhold</i>	
Bayesian Deep Learning with Multi-Spectral Inputs for Secure Crop Health Monitoring.....	619
<i>Sreelakshmi Sreeharan, Venkataramani Kumar, Jielun Zhang</i>	
Assessing Alignment of Modern AI Wearables with Trustworthy AI Requirements: A Preliminary Study.....	626
<i>Ankur Chattopadhyay, Nick Carter, Ashley Bessong</i>	
Security Triage of Flight-Critical ArduPilot and PX4 Modules with a Multi-LLM Ensemble	632
<i>Adiba Mahmud, Yasmeen Rawajfih, Ross Arnold</i>	
Keys in the Weights: Transformer Authentication using Model-Bound Latent Representations	638
<i>Ayse S. Okatan, Mustafa I. Akbas, Laxima N. Kandel, Berker Peköz</i>	
Edge-Based Collaborative Log Anomaly Detection using Retrieval-Augmented Language Models	644
<i>Daniel P. Fiadzeawu, Puhao Li, Enoch Hwang, Jielun Zhang</i>	
Seed-Induced Uniqueness in Transformer Models: Subspace Alignment Governs Subliminal Transfer	651
<i>Ayse S. Okatan, Mustafa I. Akbas, Laxima N. Kandel, Berker Peköz</i>	
Persona Vectors in Controlling Hallucination of Small Large Language Models: A Safety-Oriented Analysis.....	657
<i>Utku Kose, Ilhan Uysal</i>	
Anomaly Detection in CPS using LSTM-Autoencoder with OCSVM on SWaT Dataset.....	666
<i>Daniel P. Fiadzeawu, Derrick Agyapong, Prakash Ranganathan, Jielun Zhang</i>	
RandomFL: Randomized Federated Learning Framework for Intrusion Detection in Networked Microgrids	672
<i>Tapadhir Das, Suman Rath</i>	
Towards Intent Based Network Management: Evaluation of YANG-Based Protocols for Intent Translation.....	678
<i>Akshay R. Ramchandra, David Loper, Benjamin Blakely, Leslie Viviani, Siby J. Plathottam, Prakash Ranganathan</i>	
Breaking the Web of Lies: Closeness Centrality and the Fight Against Digital Misinformation	687
<i>Sanjaikanth E. V. S. Pillai, Wen-Chen Hu</i>	
Misinformation Hotspots: Tracking Super Spreaders by using Betweenness Centrality.....	693
<i>Sanjaikanth E. V. S. Pillai, Wen-Chen Hu</i>	
Reliability Analysis using Machine Learning for UAVs Operating Near High Voltage Transmission Lines: A State-of-the-Art Review	699
<i>Tanzim J. Hassan, Farishta Rahman, Mohammad S. Alam, Prakash Ranganathan, Hossein Salehfar</i>	

Grid Resiliency and Reliability Under Extreme Weather Events: A Systematic Review	705
<i>Mohammad Salam, Hossein Salehfar, Prakash Ranganathan</i>	
Towards Prompt and Trustworthy SoH Monitoring for Safety-Critical Battery Systems	712
<i>Mingwei Lei, Jielun Zhang, Fuhao Li</i>	
From Sensor Signals to Safety Statements: LLM-Based Justification Generation for Process Engineering	718
<i>Ifiok Udoidiok, Jielun Zhang</i>	
Improving Performance of Distributed Deep Learning in Malware and Intrusion Detection Through Relaxed Consistency	725
<i>Aavash Bhattarai, Jian Gong, Duong Nguyen</i>	
Using Machine Learning for Analysis of Consistency Faults in Distributed Computations	732
<i>Amit Garu, Duong N. Nguyen</i>	
Fail-Safe Multi-Robot Awareness During GPS Outages using CNN-Based LiDAR	740
<i>Samuel Steen, Tingjun Lei, Chaomin Luo, Guoming Li, Sicong Shao</i>	
Secure Cognitive Mapping and Neural Informed RRT* for Robust Path Planning	747
<i>Matthew Hicks, Tingjun Lei, Timothy Sellers, Chaomin Luo, Zhuming Bi</i>	
Market-Based Multi-Robot Task Allocation in Limited-Communication Environments.....	755
<i>Daniel Short, Timothy Sellers, Tingjun Lei, Jiyong Gao, Chaomin Luo</i>	
Human and AI-Generated Learning Objectives: A Comparative Study on Constructive Alignment in Secure Coding Curriculum.....	761
<i>Chizoba Ubah, Sidd Kaza, Blair Taylor</i>	
Discrete Gaussian Integer Aggregation and Trust-Budget Gating for Federated Learning in IoT-Enabled CPS.....	769
<i>Sajjad H. Shah, Mike Borowczak</i>	
Cybersecurity Bootcamp Automation and Orchestration Approaches	775
<i>David Loper, Akshay R. Ramchandra, Prakash Ranganathan</i>	
Trustworthy Cyber-Resilient Reinforcement Learning for Secure Navigation Under Adversarial Attack	784
<i>Ashwin Devanga, Tingjun Lei, Jueming Hu, Jun Chen, Chaomin Luo</i>	
Spectrogram-Based Gunshot Detection using Machine Learning Model.....	790
<i>Derrick Agyapong, Aditya Sapkota, Prakash Ranganathan</i>	
Classification of Shockwave and Muzzle Blast Signatures using CNN Models.....	797
<i>Derrick Agyapong, Jamison Jangula, Dauenbaugh Evan, Faizuddin Mohammed, Prakash Ranganathan</i>	
Prediction Models for Concrete Aging using Machine Learning	803
<i>Jaya S. R. N. Javvaji, Meera G. Sujatha, Iraj H. P. Mamaghani, Prakash Ranganathan</i>	
Scalable Streaming Architecture for Threat Analytics.....	813
<i>Shubham Amilkanthwar, Snahil Singh, Priyank Desai</i>	
The Science of Threat Modeling in Complex Industrial Systems	818
<i>Snahil Singh, Priyank Desai, Shubham Amilkanthwar</i>	

Comparative Evaluation of Machine Learning Models for Classifying Operations and Attacks in Distributed Energy Resources	825
<i>Nikola Petrovic, Luka Strezoski, Dejan Milojevic, Cullen Bash</i>	
A Survey of Large Language Models for Insider Threat Detection.....	834
<i>Ali Haidar, Yu-Zheng Lin, Qinxuan Shi, Zhanglong Yang, Desmond Amadigwe, Brian Terry, Sudheer K. Battu, Pratik Satam, Sicong Shao</i>	
Deep Ensemble-Based Insider Threat Detection Dealing with Small Data.....	844
<i>Desmond Amadigwe, Qinxuan Shi, Zhanglong Yang, Preeti Choubey, Ali Haidar, Sicong Shao, Tingjun Lei, Weiyang Zhang</i>	
Evaluation of Foundation Models for Infrastructure-as-Code Automation on Amazon Bedrock	851
<i>Brian Terry, Qinxuan Shi, Zhanglong Yang, Ali Haidar, Sicong Shao</i>	
A Survey on Man-in-the-Middle Attacks in Distributed Energy Resources (DER) and Industrial Control System(ICS) Environments	858
<i>Shree R. A. Balaji, Prakash Ranganathan</i>	
A Hybrid Approach to Malware Detection: Integrating Few-Shot Model-Agnostic Meta-Learning with Autoencoders	868
<i>Emmanuela Andam, Yasir A. Zaidi, Abdelali Hadir, Emmanuel Grant, Naima Kaabouch</i>	
Towards Explainable Federated Intrusion Detection for IoT in Resource-Constrained Environments	876
<i>Charles Stolz, Jielun Zhang</i>	
When Disasters Trigger Cyber Vulnerabilities: Mapping Physical-Digital Interdependencies in Critical Infrastructure Systems	882
<i>Dikshya Panta, Sicheng Wang, Aditya Sapkota, Prakash Ranganathan</i>	
Real-Time Analysis of DDoS Attack Detection and Mitigation Measures using XGBoost Machine Learning Algorithm	893
<i>Seth Y. Alornyo, Derrick Agyapong, Joel K. Kibiwott, Eunjin Kim</i>	
A Survey of Adversarial Machine Learning Attacks in Unmanned Aircraft System Traffic Management	900
<i>Qinxuan Shi, Toro D. Caleb, Sicong Shao, Naima Kaabouch</i>	

Author Index