

2025 IEEE International Carnahan Conference on Security Technology (ICCST 2025)

**San Antonio, Texas, USA
13-17 October 2025**

IEEE Catalog Number:
ISBN:

CFP25ICR-POD
979-8-3315-2320-6



Copyright © 2025, IEEE

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:	CFP25ICR-POD
ISBN (Print-On-Demand):	979-8-3315-2320-6
ISBN (Online):	979-8-3315-2319-0

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

TABLE OF CONTENTS

Explainable Bidirectional LSTM Autoencoder for Insider Threat Detection in Various Scenarios	1
<i>Abdul Muqtadir Abbasi, Fariha Muqtadir, Otman Basir, Shi Cao</i>	
Explicit Behavioral Embedding Method for Generating Explanations of Insider Threat Events	7
<i>Abdul Muqtadir Abbasi, Fariha Muqtadir, Otman Basir, Shi Cao</i>	
Technical Risk Indicators for the Critical Pathway to Insider Risk	13
<i>William R. Claycomb, Daniel L. Costa</i>	
A Novel Approach for Host-Based Security: SecureHost IDS	18
<i>Natalie Rankin, Ayad Barsoum</i>	
A Novel Vulnerability Prioritization Model for Workstation Endpoints with Context Intelligence	24
<i>Logan Scott, Jeremy Cohen</i>	
Anomaly Detection Using Multivariate Gaussian Analysis on Communication Networks	30
<i>Donald Van Rheeden, Benjamin Holladay, Chenchen J. Li</i>	
Interpreting CNN in Cybersecurity: Process-Level Attribution via Benign-Replacement Occlusion (BRO)	35
<i>Gavin Holliday, Randall Klepetko</i>	
Assessing Software Security Maturity via an AI-Augmented Risk-Based Framework	41
<i>Han W. Lin, William M.S. Stout, Tyler J. Morris</i>	
AI-Powered Intrusion Detection with SHAP Explainability and Feedback Loop: A Modular Pipeline for Cyber Threat Classification	47
<i>Raj Kumar Myakala, Akhil Reddy Jagirapu, Vinithya Reddy Podduturi, Praveen Kumar Nagata Sampath Lavudya, Sanjeev Kumar Pedhapally</i>	
Risk Profiling of CVE Vulnerabilities via Unsupervised Clustering	53
<i>Arbaz Surti</i>	
Lightweight AI-Based Intrusion Detection Models for IoT Devices: A Comparative Review	59
<i>Abhineeth Pasam, Ahaan Sinha, Akalanka Mailewa</i>	
A Risk-Conscious Cybersecurity for Healthcare via Zebra-Inspired Optimization of Machine Learning Models*	66
<i>Damodhara Reddy Palavali, Suneetha Pothireddy</i>	
Adversarial Attacks on FinTech AI Models: Threats and Mitigation Techniques	72
<i>Veeramani Sampathkumar, Krishaa Veeras</i>	
Efficient Backdoor Defense for Federated Learning with Partial Model Inspection	79
<i>Kyle Wilkerson, Palden Lama, Andrew Mellow, Ryan Bonnet, Vasudha Vedula, Rajendra Boppa</i>	
Quantum GAN-Based Adversarial Attack Generation for Network Intrusion Detection System	85
<i>Ishan Prashant Pathak, Nuri Yilmazer, Darshan Pankajkumar Patel</i>	
Post-Quantum Cryptography on Constrained Networks	91
<i>Seth Smith, Kyle Owens, Katherine Kozan</i>	

VeriPhish: Bridging AI Explainability and Accuracy in Phishing Detection Through XAI and LLMs	95
<i>Panhapiseth Lim, Roman Huerta, Alejandro Sotelo, Anthonie Quintela, Martin Husák, Priyanka Kumar</i>	
Redefining Cyber Resilience: AI-Driven Metrics for Enhanced Threat Intelligence Systems	101
<i>Esther Eze, Gahangir Hossain</i>	
AI-Driven Real-Time API Security: Explainable Threat Detection for Cloud Environments	108
<i>Akshay Mittal, Pragya Keshap, Arpana Hosabettu</i>	
Robust Federated Learning via Stable Cosine Similarity	115
<i>Rakib Ul Haque, Panagiotis Markopoulos</i>	
Enhancing a Moving Target Defense Solution for IoT Agents with Task Distribution	121
<i>Augusto Morales</i>	
AI-Powered IoT Security: Multi-Dataset Evaluation of a Deep Learning Intrusion Detection Framework	127
<i>Salahaldeen Duraibi, Saahira banu Ahamed, A.Salman Maricar</i>	
Adaptive Dual-Agent Authentication Framework: Balancing Security and user Experience in Digital Banking	133
<i>Akshay Mittal, Sabarinathan Govindaraj</i>	
Securing the Next-Generation IoT: An Integrated Security Framework with AI, Blockchain, and Edge Computing	139
<i>Akshay Mittal, Tharun Anand Reddy Sure</i>	
Cybersecurity in Smart Transit Infrastructure: A Meta-Review of Technical and Socio-Organizational Gaps	144
<i>Bryan Anderson, Gahangir Hossain</i>	
Autonomous UAS Object Avoidance and Path Detection Using Neuromorphic Computing	151
<i>Brian Millikan, Lauren Reinerman-Jones, Daniel Barber</i>	
Coreference Pattern-Aware Intelligent Text Watermarking Scheme for Forensic Identification Via Improved Deep Learning Approach	155
<i>Akhil Vaitla Janardhan</i>	
Spiking Neural Networks for RF Signal Classification and Unified Timing Estimation on Loihi 2	161
<i>Howard Yanxon, Lauren Reinerman-Jones</i>	
The Role of Psychoeducation for Stress Reduction in Security Management - The Case Study of Pompeii Archaeological Park	165
<i>Fabio Garzia, Francesco Borghini, Alberto Bruni</i>	
A New Hybrid Steganographic Technique for MP3 File	171
<i>Fabio Garzia, Roberto Cusani, Roberta Penniello</i>	
AI-Driven Digital Twin Framework for Security Threat Simulation and Compliance Optimization	177
<i>Vivek Venkatesan, Chakkaravarthy Arunachalam</i>	
Exposing and Mitigating Adversarial AI Threats in IoT/5G Intrusion Detection Systems Using Random Forest and Feature Reduction	183
<i>Harika Rama Tulasi Karatapu, Shafeeq Ur Rahaman, Sudheer Patchipulusu</i>	

The Role of Velocity in Online Signature Verification: Security Concerns	191
<i>Cristian Rodriguez, Moises Diaz, Jose Francisco Lorenzo, Miguel A. Ferrer</i>	
Machine Learning for Digital Signatures	197
<i>Juan Ortiz Couder, Lynn Vonderhaar, Omar Ochoa</i>	
Is One View Enough - Biomatter Threat Identification in 3D CT Scans	203
<i>Ivan Koptev, Cameron Walker, Andreas W. Kempa-Liehr</i>	
Knowledge, Mental Models, and Trust Regarding AI for Baggage Screening	209
<i>Giulio Staufer, Adrian Schwaninger, Yanik Sterchi</i>	
A New Fairness Evaluation Metric of Biometric Systems Based on the Theil Inequality	215
<i>Kaira Neily Sanon, Joël Di Manno, Christophe Charrier, Christophe Rosenberger</i>	
Explainable Ai(Xai) for Touch-Stroke Biometrics: Insights from Shap	221
<i>Soodamani Ramalingam, Dominic Lovric, Ooi Shih Yin, Richard Guest, Moises Diaz, Fabio Garzia</i> <i>David Lawunmi</i>	
Studying the Generalized Coordinates and Torques in On-Line Signature Verification	227
<i>Moises Diaz, Miguel A. Ferrer, Cristian Rodriguez, Jose Francisco Lorenzo, Juan M. Gil, Rafael Rodriguez</i>	
Hard-Earned Lessons in Access Control at Scale: Enforcing Identity and Policy Across Trust Boundaries with Reverse Proxies and mTLS	232
<i>Mitendra Kumar Mahto, Sanjay Singh</i>	
Zero Trust and Cyber Risk Modeling for Intelligent School Transportation Systems (ISTS)	238
<i>Prashant Vajpayee, Bryan Anderson, Gahangir Hossain</i>	
Features Analysis of All Email Components for Phishing Detection	244
<i>Armand Florent Tsafack Piugie, Mathieu Valois, Emmanuel Giguët, Philippe Chauvat</i> <i>Christophe Rosenberger</i>	
The Public Chatter Bureau - A Framework for Cyber Threat Early Detection and Triage	250
<i>Dippu Kumar Singh</i>	
The Evolution of Secure Access Service Edge in the Digital Landscape: Comprehensive Literature Review	258
<i>Vishal Gudhka</i>	
Logic Locking for Protecting Sensitive Microelectronics: Perspective and Analysis	266
<i>Jason Hamlet, Jonathan Cruz</i>	
A Strategic Position on Multi-Agent AI Systems for Secure and Scalable Retail Fraud Detection	273
<i>Jay Prakash Thakur, Akshata Kishor Moharir, Ananya Ghosh Chowdhury</i>	
FedScam-NBD: Federated Learning for Network Behavior-Driven Telecommunication Scam Detection	280
<i>Laxmi Shaw, Ganesh Gaiy, Tahir Ekin</i>	
Exploring the Integration of Edge AI into 6G Networks: Implications for Network Efficiency, Security, and Privacy	286
<i>Muzibur Rahman Rukon, Ridma Hoq, Mehek Hasnat</i>	
Formal Verification of LSQ-LFENCE for Memory Ordering and Security Assurance	290
<i>Chukwunalu Asuai, Kushal K. Ponugoti</i>	