2025 International Conference on Cybersecurity and AI-Based Systems (Cyber-AI 2025)

Varna, Bulgaria
1-4 September 2025

IEEE

IEEE Catalog Number: CFP250Q0-POD
ISBN: 979-8-3315-6632-6

****** 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:	CFP250Q0-POD
ISBN (Print-On-Demand):	979-8-3315-6632-6
ISBN (Online):	979-8-3315-6631-9

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

A Study of Cybersecurity in the Healthcare Sector: Threat and Vulnerability Mapping 1
Marcel Puşcaşu, Mihai Dimian, Doru Balan, Timofte Edi Marian, Daniel-Florin Hriţcan

AI-Generated Text Steganography - Hiding Secrets in Plain Sight Using Synonym Encoding 9
Petar Stoilov, Plamen Zahariev

Large Language Models for Toxic Language Detection in Low-Resource Balkan Languages 14
Amel Muminovic, Amela Kadric Muminovic

FATEEN: An AI-Empowered Floating IoT System for Enhancing Toddler Pool Safety 22
Fatima Albaity, Alia Alkaabi, Mariam Almakhzoumi, Mariam Aldhaheri, Mozah Alhefeiti, Abdulmalik Alwarafy

Cyberbullying Detection: A Comparative Evaluation of Learning Models on a Unified Public Dataset 28
Diana Ghanem, Daoud Mansour, Raghad AlSayeh, Zaid Amari, Ayat Hamzah, Majdi Maabreh

DarkWatchAI - Unsupervised Machine Learning for Identifying Fintech Threats in DarkWeb Posts 34
Luiza Nacshon, Abhishek Tatti, Dan Poremba, Jordan Garzon

LLMs for Penetration Testing: Solving CTF Challenges Using Offensive Cybersecurity Tools 43
Erik Adler, Johannes F. Loevenich, Florian Spelter, Tobias Hürten, Damian Roncevic, Maxime Schwarzer, Roberto Rigolin F. Lopes

A Secure Threat Detection Framework for Federated Learning in Healthcare Environments 51
Preksha Joshi, Sneh Singh

Artificial Intelligence and Islamic Jurisprudence: Ethical, Legal, and Theological Considerations 59
Reema Al Qaruty, Suha AlQaruty, Khawlah M. AL-Tkhayneh, Samer Abdel Hadi

Efficient Hybrid Model for Ransomware Detection Using Machine Learning Techniques 67
Shorouq Al-Eidi, Omar Khadrawi, Manal Alhathli, Omar Darwish

Optimized Detection of SQL Injection Attacks Using Machine Learning: Enhancing Accuracy and Explainability in Cybersecurity 73
Wael A. AlZoubi, Sanaa Mohsin, Abdulghafor M. Hashim, Ahmed D. Radhi, Zainab G. Alrashid, Emad A. Az-Zo'Bi, Mohammad A. Tashtoush

A Ransomware Resilience Method with LLM-Driven Threat Intelligence 82
Syed Sohaib Karim, Waseem Iqbal, Farooq Zaman, Imran Rashid, Dawood Al-Abri

Efficacy of Spiking Neural Networks for Intrusion Detection Systems 89
Leonard Knapp, Sven Nitzsche, Matthias Börsig, Alexandru Vasilache, Ingmar Baumgart, Juergen Becker

Sentiment Analysis of Tweets Using Machine Learning and Deep Learning Models: A Comparative Study 96
Abdallah Al-Shorman, Omar Darwish

Efficient End-To-End Intrusion Detection with Packet and Flow-Level Mamba Sequence Models 103
Benedikt Pletzer, Jürgen Mottok

A Deep Learning-Supported Framework for Estimating Inverse Rayleigh NHPP Parameters in Critical Infrastructure 111
Rana N. Abbas, Shaimaa W. Mahmood, Adel S. Hussain, Ahmed D. Radhi, Abdulghafor M. Hashim, Emad A. Az-Zo'bi, Mohammad A. Tashtoush

Innovative Model for Development and Technology Commercialisation of Technological Innovations 118
Sia Tsolova

Intelligent Intrusion Detection in IoT with Explainable AI and Distributed Web Systems 124
Marian Ileana, Pavel Petrov, Vassil Milev

Detection of Malicious Executable Files Using Hybrid Feature Based on Data Mining Techniques..... 128
Enas Al Shrida, Yahya Tashtoush, Ghaidaa Al sheikh, Areej Al Zoubi, Mohsen Mohaidat, Ali Alqahtani

Securing Internet-Of-Things Using Machine Learning: A Survey 136
Ali K. Jaber, Mohammed M. Alani

Analyzing Student Behavior from Moodle Data Using Process Mining and Deep Learning 143
Rami Abu Agolah, Malak Abdullah, Alex Mircoli, Mahmoud Al-Ayyoub, Dana Elrushaidat

Enhancing Image Classification Through Adaptive Image Resizing 149
AbedlRahman Almodawar, Ashraf Ahmad, Plamen Zahariev, Yahya Tashtoush

Layered Machine Learning for Scalable Intrusion Detection in IoT Healthcare Systems..... 156
Dana El Rushaidat, Batool Alkhalil, Tuqa Sammak, Yumna Ghannam

Evaluating the Impact of an International Cybersecurity Camp on Participants' Skills, Knowledge, and Collaboration 163
Muhammad Mudassar Yamin, Birgy Lorenz

Detecting Anomaly Attacks in Software Defined Networking Using Machine Learning with Feature Selection Method..... 170
Firas Al Balas, Dalya Al.Nore, Crenguța-Ileana Sinisi, Loredana Maria Păunescu

Multi-Layer Grad-CAM (MLGC) Explainable AI Model for Texture Prediction..... 175
AbedlRahman Almodawar, Ashraf Ahmad, Georgi Hristov, Yahya Tashtoush

Agentic Penetration Testing Using Secure Shell: Context-Aware Command Generation and Analysis Using Open-Source LLMs..... 182
Siddhant Prashant Kale, Preet Kanwal, Prasad B Honnavalli

Lightweight Federated Knowledge Distillation with Adaptive Pruning and Privacy..... 190
Asaad Althoubi

Improving Intrusion Detection System Accuracy Through PCA-Based Feature Reduction and Machine Learning Techniques..... 198
Amer Mosally

The National Identity in the Digital Media Discourse on Twitter: Insights from NodeXL 204
Dina Tahat, Najia Ketbi, Noura Naqbi, Sara AlMaleki, Abdulaziz Altawil, Khalaf Tahat, Baghdad Alshanaq

PSNR-Based Adaptive Image Padding for Image Classification-Specific Tasks 210
AbedlRahman Almodawar, Ashraf Ahmad, Nayef Alqahtani

The Practical Impact of AI on Green Logistics: The Mediating Role of Sustainability Practices in Transportation Sector in Jordan 216
Firas Tayseer Ayasrah, Ahmad Y. A. Bani Ahmad, Mahmoud Allahham, Wasef Ibrahim Almajali, Hamzeh Alhawamdeh, Dony Novaliendry, Irwanto Irwanto

Compact and Effective: Lightweight Machine Learning Models for DDoS Attack Detection 226
Majdi Maabreh, Mohammad Dabash, Ahmad Musleh, Noha Mahmoud, Dana Al-Nadi

A Comparative Study on Malware Detection Using Supervised Machine Learning Models 232
Irfan Mohammed, Shahzad Memon, Umar Mukhtar Ismail

Exploring Technological Innovations in Digital Supply Chain Management: The Mediating Role of Artificial Intelligence 237
Firas Tayseer Ayasrah, Mahmoud Allahham, Wasef Ibrahim Almajali, Ahmad Y. A. Bani Ahmad, Najwa Mohammad Ashal, Febri Prasetya, Aprilla Fortuna

Key Characteristics of Educational Video Games for STEM Education - A Literature Review 248
Stanislav Ivanov, Nikolina Nikolova, Borislav Yordanov, Boyan Bontchev

Federated Multi-Agent Deep Reinforcement Learning for Task Offloading and Resource Allocation in Multi-WBAN MEC Systems 256
Heba M. Khater, Farag Sallabi, Ezedin Barka, Mohamed Adel Serhani

CAT-GPT-4: Context-Aware Phishing Detection with Explainability 262
Asaad Althoubi

Time-Series AI Models for Detecting Stealthy DNS Flood Attacks 270
Taiwo Olawuni, Olayemi Olawumi, Yang Li, Ameer Al-Nemrat

Failure Modeling in Intelligent Systems: Toward Reliable and Trustworthy AI Components 278
Sanaa Mohsin, Zainab G. Alrashid, Hasanain J. Alsaedi, Wael A. AlZoubi, Adel S. Hussain, Emad A. Az-Zo'bi, Mohammad A. Tashtoush

Real-Time AI-Driven 6D Pose Estimation for Robotic Picking in Cluttered Bins Via Two-Stage Segmentation and CAD-Guided Alignment 285
Simeon Tsvetanov, Teodor Boyadzhiev, Denis Chikurtev

Comparing Machine Learning and Deep Learning Models for QR Code Phishing Detection 291
Yahya Tashtoush, Mahar Khashim, Nasser Alsaedi

An Improved Tweet Classifier with a Hybrid Text and Graph-Based Representation 298
Ola Karajeh, Lamya Abdullah, Nasser Alsaedi, Anas Alsobeh, Omar Darwish

An AI-Driven Framework for Agricultural Data Interoperability Informed by Literature and Stakeholder Insights 308
Fjolla Berisha, Leidiane Da Silva, Erica Tegolo, Peter Mooney, Zohreh Pourzolfaghar, Markus Helfert

ShadowPlay: Engineering Defenses Against Role-Based Prompt Injection and Dependency Hallucination in LLM-Powered Development 317
Anas AlSobeh, Zahraddeen Gwarzo, Amani Shatnawi

Leveraging Large Language Models for Detection and Intelligent Analysis of Phishing Threats 326
Yahya Tashtoush, Mona Al-Nemrawi, Leen Masa'Deh, Ban Al-Qudah, Saeed Alqahtani

On Technique Identification and Threat-Actor Attribution Using LLMs and Embedding Models 332
Kyla Guru, Robert J. Moss, Mykel J. Kochenderfer

Specification and Evaluation of Multi-Agent LLM Systems - Prototype and Cybersecurity Applications..... 340
Felix Härer

Author Index