

2026 14th International Symposium on Digital Forensics and Security (ISDFS 2026)

**Boston, Massachusetts, USA
19-20 March 2026**

Pages 1–605

IEEE Catalog Number: CFP26F05-POD
ISBN: 979-8-3315-7311-9



Copyright © 2026, 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:	CFP26F05-POD
ISBN (Print-On-Demand):	979-8-3315-7311-9
ISBN (Online):	979-8-3315-7310-2
ISSN:	2837-827X

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

Forensic Investigation of SDRSharp and RTL-SDR Dongle in Eavesdropping Radio Communications	1
<i>Erasmus Mfodwo, Narasimha Shashidhar, Cihan Varol, Ahmet Furkan Aydogan</i>	
BICIR: A Blockchain-Based Interoperability Model for Cross-National Cyber Incidents	8
<i>Osayomore O. Aigbogun, Cihan Varol</i>	
Two Pillars of Banking Intelligence: A Comparative Analysis of AI Techniques for Fraud Prevention and Churn Mitigation	15
<i>Sreenivasulu Gajula</i>	
Thermal Imaging and Convolutional Neural Nets for Advanced Warning of Fires on Critical Data Infrastructure	21
<i>Steven May, Cihan Varol</i>	
Video Streaming Over Vehicular Ad Hoc Networks: A Review	26
<i>Omer Mohammed Salih Hassan, Ismail Amin Ali, Asaf Varol</i>	
R v F (2025): Addressing the Defence of Hacking	34
<i>Junade Ali</i>	
Comparative Analysis of Cybersecurity Law and Warfare in the United States (CCPA) and Europe (GDPR): A Pre2020 vs Post-2020 Perspective	38
<i>Martina Kalu, Cihan Varol</i>	
AI-Powered Android Immune System: A Hybrid Static and Semantic Model for Malware Neutralization	45
<i>Mohd Fozla Rabby</i>	
VANET Simulators:An Overview and Comparative Analysis	51
<i>Omer Mohammed Salih Hassan, Ismail Amin Ali, Asaf Varol</i>	
An Information Asymmetry Game for Trigger-Based DNN Model Watermarking	58
<i>Chaoyue Huang, Gejian Zhao, Hanzhou Wu, Zhihua Xia, Asad Malik</i>	
Weakly Supervised Knowledge Base Construction for Telegram Gift-Card Fraud Messages	64
<i>Chunlan Gao, Yubao Wu</i>	
Optimizing Resistive Losses in Transmission Systems Via Voltage Level Selection	70
<i>Kendall D. Standridge-Monroe, Asaf Varol</i>	
Explainable Customer Lifetime Value for Personalized Enterprise Resource Planning Strategy and Intervention	78
<i>Vinay Singh, Prashant Gupta, DhirajKumar Pathak</i>	
SQL Vs. NoSQL Comparative Analysis of Database Management Systems for Scalability and Performance	86
<i>Ravi Sankar Susarla, Viswa Bharath Kolla</i>	
A Lightweight Hybrid Temporal CNN-Transformer Architecture for Real-Time Healthcare Anomaly Detection on Wearables	93
<i>Akshit Naithani, Vrishin Jain</i>	

Weak Enforcement and Low Compliance in PCI DSS: A Comparative Security Study	99
<i>Soonwon Park, John D. Hastings</i>	
safeMEDInet: Fed AI Systems for Privacy-Preserving Threat Detection in Healthcare	105
<i>Irin Sultana, Syed Mustavi Maheen, Naresh Kshetri, Shriram KS Pandian, Marshiat Mithe Syed Md Rasel Ahmed</i>	
ppAIsec: Privacy-Preserving AI Models in Healthcare Security - AI Frameworks Synthesis	112
<i>Tanzina Sultana, Asura Akter Sunna, Mohammed Majbah Uddin, Naresh Kshetri</i>	
Comparative Analysis of Steganography Injection and Detection Tools/Methods: Traditional vs. AI-Based	118
<i>Rahaf Alnuaimi, Maryam Almarzooqi, Farkhund Iqbal</i>	
Design and Analysis of Energy Efficient ASCON 80Pq	126
<i>Ananthraj Rao Kekuda, Anirudh G P, Ashwin Thomas, Srinivasa V S Sarma D</i>	
Deterministic LLMs: a Practical Forensic Framework for Verifiable and Reproducible Local LLM Inference	131
<i>Joel D. Molina</i>	
Interpretable Ensemble Learning for Network Traffic Anomaly Detection: A Shap-Based Explainable AI Framework for Embedded Systems Security	137
<i>Wanru Shao</i>	
Analyzing the Effects of Prompt Styles on Large Language Model Chatbot Responses	141
<i>Niloofar Kolahchi, Michael W. Totaro</i>	
GenReachAI: An Agentic Generative AI Framework for Automated Reachability Analysis of Enterprise Software Vulnerabilities	147
<i>Niranjan Pachaiyappan</i>	
Explainable Risk Decision Systems Using Artificial Intelligence Models for Payment Fraud Identification with Mitigation	154
<i>Dilip Patel</i>	
From Cracks to Crooks: YouTube as a Vector for Malware Distribution	160
<i>Iman Vakilinia</i>	
Proof-by-Asset: A Blockchain-Backed Model for Asset-Based Authentication	166
<i>Zoé Elliott, Iman Vakilinia</i>	
Stability Analysis of Synchronous Generator Systems Under Variable Load Conditions	172
<i>Brenden Lippard, Chase Guttu, Asaf Varol</i>	
A Systematization of Privacy Threats and Defenses in Modern Agentic Web Browsers	177
<i>Niranjan Pachaiyappan</i>	
Fragility of Children's Online Privacy	182
<i>Abdulbast Abushgra, Adam Keeling, Jesse Caudell, Ada Johnson, Jayden Bowman, Magan Miller</i>	
From Monolithic Middleware to Cloud-Native Microservices: a Performance-Driven Modernization Study	187
<i>Sauhard Bhatt</i>	

Achieving 60% Diesel Reduction at Music Festivals Through Intelligent Load Segmentation	193
<i>Robert Owens, Asaf Varol</i>	
Deep Learning-Based Intrusion Detection and Cybersecurity Framework for Connected Vehicle CAN Bus Communication Networks	199
<i>Shiva Kumara, Henry P Cyril</i>	
Thorax Disease Classification Based on Spatial Transformer Networks and Squeeze-and-Excitation Blocks	205
<i>K Jenni, Nala ALAhmari, G Aniruth, M Srinivas</i>	
An Effective System for Medical Image Diagnosis Using Deep Convolutional Networks (CNNs) in Healthcare Sector	211
<i>Sanjoy Mukherjee</i>	
AI-Driven Self-Healing and Intelligent Queuing Through Anomaly Detection in 5G Cellular Networks	217
<i>Henry P Cyril</i>	
Improved Prostate Zonal Segmentation: Addressing the Peripheral Zone Challenge Via a Peripheral-Centric Swinunet	223
<i>Abidus Sattar Aziz, Md Masum Rana, Yousuf Abdullah Borna, Md Rezwanul Akter Pallab, Plato Chakma</i>	
Vision Transformer for Epilepsy Seizure Prediction and Detection: A Narrative Review	229
<i>Md Masum Rana, Abidus Sattar Aziz, Md Rezwanul Akter Pallab, Yousuf Abdullah Borna</i>	
Compute-Optimal Resource Allocation for Distributed Large Language Model Inference in Cloud-Scale Intelligent Systems	235
<i>Tejas Pravinbhai Patel, Sandeep Shivam, Viswanathan Ranganathan</i>	
Explainable and Human-Centric Approaches in Audio Steganalysis: A Review	241
<i>Sarah Rahim, Guhanathan Poravi</i>	
TrustFed-He: Trustworthy Federated Fraud Analytics for Banks with Homomorphic Secure Aggregation and Poisoning-Resilient Training	247
<i>Srikumar Nayak</i>	
Enhancing Early Diabetes Screening Through Machine Learning and Explainable AI	254
<i>Jahnvi Anilkumar Kachhia</i>	
Secure and Privacy-Preserving Healthcare Federated Learning via Differential Privacy Mechanisms	260
<i>Maunik K Shah, Munir Rajesh Mehta</i>	
Intelligent Data Integration and Analytics for Automotive Aftermarket Retail: An Informatica-BigQuery-Tableau Framework	266
<i>Rambabu Tangirala</i>	
Distributed Adaptive Speculative Decoding: Accelerating Large Language Model Inference With Context-Aware Draft Selection	272
<i>Tejas Pravinbhai Patel, Vinay R Soni, Amit Kumar Padhy, Siva Rama Krishna Varma Bayyavarapu Milan Parikh</i>	
Modernizing SAP Business Objects Using Enterprise Data Warehousing Principles	278
<i>Prasanth Sathyapalan</i>	

AI-Enhanced Digital Forensics: A Research Vision for Trustworthy, Explainable, and Humancentered Forensic Intelligence	284
<i>Nadeem Daudpota</i>	
FAKE-OT: An Open Architecture for Threat Detection in OT Environments Using MQTT-Based Honey pots	289
<i>Hebert Silva, Felipe Carvalho, Tiago Demay</i>	
Normalizing Flow for Financial Anomaly Detection: the Impact of Loss Function	295
<i>Amir Rashidi, Ruobin Qi, Rashida Hasan</i>	
Operationalizing Data Economy in Data Spaces: A Token-Based Reference Implementation	301
<i>Muhammed Turkanović, Martin Ferenec, Teo Lah, Vid Keršič</i>	
A Formal Model of Access Token Bifurcation and Integrity-Based Isolation in Windows Kernel Architectures	307
<i>Jean Rosemond Dora, Ladislav Hluchy</i>	
Windows Operating System Credentials - Elevation with Impersonation	313
<i>Jean Rosemond Dora, Ladislav Hluchy</i>	
Security Architecture of Kerberos Authentication and Domain Credential Management	319
<i>Jean Rosemond Dora, Ladislav Hluchy</i>	
A Comparative Analysis of URL Features for Machine Learning Phishing Detection	325
<i>Chukwunali Asuai, Yusuf Moshood</i>	
Machine-Learning Driven Performance Modeling and Optimization of Probabilistic and Hardware Accelerators	331
<i>Uday Korat, Mitesh Patel</i>	
BHF-Guard: Breaking and Hardening Financial ML with Adversarial Stress Tests and Certified Robustness Checks	337
<i>Srikumar Nayak</i>	
Explainable Risk Decision Systems Using Artificial Intelligence Models for Payment Fraud Detection and Identification	344
<i>Deepak Reddy Suram</i>	
Transformer Based Framework for Imbalanced Transaction Fraud Detection in FinTech Systems	350
<i>Sandeep Shivam, Venkat Nutalapati, Tejas Pravinbhai Patel, Amit Kumar Padhy, Madhushree Kumari Rajesh Purushothaman</i>	
An Experimental Study of Linux Landlock: File-System Enforcement Behavior and Overhead	356
<i>Harsh Deepak Singh, Michael J. Dinneen, Sathiamoorthy Manoharan</i>	
Design and Development of an Artificial Intelligence—supported Educational Portal with Role-Based Authorization Structure	362
<i>Songul Karabatak, Muslim Alanoglu, Murat Karabatak, Beyza Basatoğrul</i>	
NeuroShield: A Temporal Spike Timing Attack Detection Framework for STDP Based Neuromorphic Systems in Multi-Cloud Environments	368
<i>Naga Sujitha Vummaneni, Sundeep Bobba, Akhil Peddi</i>	

Evaluating the Vulnerability of Deepfake Image Detection Models to Adversarial Manipulations	374
<i>Prakriti Shakya, Katya Mkrtchyan, Rashida Hasan</i>	
Zero Trust Architecture for 5G-Enabled Mobile Cloud Computing (MCC)	380
<i>Urvish Pandya, Sweta Pandya</i>	
Securing Unmanned Aerial Vehicles: Addressing Cyber Threats and Vulnerabilities in UAVs Systems	386
<i>Jaber El Mahjoub, Abderrahim Abdellaoui</i>	
Optimizing Post-Quantum Cryptographic Algorithms for Resource-Constrained Devices	394
<i>Sai Charan Reddy Nevuri</i>	
Enhancing Post-Quantum KEMs: A Secure and Efficient Transformation	402
<i>Sai Charan Reddy Nevuri</i>	
Performance Evaluation of Post-Quantum Cryptography in IoT: A Case Study on MQTT Over TLS Under Network Constraints	408
<i>Emerson Costa Santos, Tiago Augusto Orcajo Demay Cordeiro, Hebert de Oliveira Silva</i>	
The Investigation of the Relationship between Peer Relationships and Internet Addiction Levels of High School Students	414
<i>Merve Özer, Ayşenur Kuloğlu, Müslim Alanoğlu, Murat Karabatak</i>	
Enhancing Indoor Localization Accuracy with Bluetooth Low Energy RSSI Signals Analysis Using Machine Learning Algorithms	419
<i>Mitesh Patel, Uday Korat</i>	
InfotainPC: Exploring the Privacy Concerns Within in-Vehicle Infotainment Data Services Using TAM	425
<i>Samiul Alam</i>	
Empirical Analysis of AI Confidence Methods in Digital Forensic Standards	431
<i>Milinda Rambel Stone, Varghese Vaidyan</i>	
Hardening the OSv Unikernel With Efficient Address Randomization: Design and Performance Evaluation	437
<i>Alex Wollman, John Hastings</i>	
Nowhere to Hide: Comparative Analysis of Residential Vs. Cloud Attack Surfaces	443
<i>Sankalp Lanka, Om Palsule, Rishik Lanka, Phani Lanka</i>	
Database Forensics Readiness: An Examination of Redis	449
<i>Muhammad Abdul Moiz Zia, Oluwasola Mary Adedayo</i>	
Enforcing Accountability in Autonomous Ops: A Zero-Trust Multi-Agent Framework With Forensic Reasoning Ledgers	456
<i>Madhvesh Kumar, Deepika Singh</i>	
Research Study on AI-Driven Weapon and Violence Detection in Smart Cities	463
<i>Thangavel Murugan, Anoud Salem Alkarbi, Maryam Ahmed Alzeyoudi, Noura Ali Matar Alketbi Afra Khaleifah Alteneiji, N. Nasurudeen Ahamed</i>	
Microarchitectural Espionage: FPGA-Based Security Analysis of Branch Prediction in RISC-V Out-of-Order Cores	469
<i>Mahreen Khan, Muhammad Emir Bin Mohd Shahfie, Maria Mushtaq, Renaud Pacalet, Ludovic Apvrille</i>	

Network Hardening Based on Companion Planting in Iot Environments with Unknown-Vulnerability Devices	476
<i>Shingo Yamaguchi</i>	
Data-Driven AI Techniques in Raman Spectroscopy for Biomedical Applications: A Comprehensive Review	482
<i>Shahbaz Ahmed, Muhammad Raheel Raza, Asaf Varol</i>	
A Hybrid Approach to Detect Illegal Activities in Dark Web Data	488
<i>Akash G Gaonkar, Abhinav V P, Aditya V Bhat, Jeny Jijo, Abishek K</i>	
Development of an Artificial Intelligence-Supported Mobile Learning Application	494
<i>Songül Karabatak, Muslim Alanoğlu, Ayşenur Kuloğlu, Dilara Sucu</i>	
The Need for Standardized Evidence Sampling in CMMC Assessments: A Survey-Based Analysis of Assessor Practices	499
<i>Logan Therrien, John Hastings</i>	
Forensic Event Reconstruction of Web Attacks Using Log Decoder and Rule-Based Correlation	505
<i>Muhammad Nur Yasir Utomo, Hudan Studiawan, Baskoro Adi Pratomo</i>	
go-safeinput: A Zero-Dependency Input Sanitization Framework for Digital Forensics and Cybersecurity Applications	511
<i>Ravi Sastry Kadali</i>	
Design of a Web-Based Modular Self-Assessment System for Education Portals	517
<i>Songül Karabatak, Müslim Alanoğlu, Meltem Yurtçu, Süleyman Polat</i>	
Quantum-Safe Countermeasures: Mitigating Detector-Blinding Attacks in Quantum Key Distribution Systems	523
<i>Wail Zita, Malek Malkawi</i>	
AI-Enhanced Cybersecurity Risk Assessment for Smart Grid Infrastructures Using NIST Framework	529
<i>Hala Strohmier Berry, Yash N Dasri, Soumik Mitra, Bhargav Palaskar</i>	
Chacha20-E: An Improved Chacha Algorithm for Secure Data Transmission on IoMT Devices	538
<i>Jabari Khawla, Abdellaoui Abderrahim</i>	
LRD-Net: A Lightweight Real-Centered Detection Network for Cross-Domain Face Forgery Detection	544
<i>Xuecen Zhang, Vipin Chaudhary</i>	
Token-Based Authentication System Failures in Cloud Environments: A Case Study of the Microsoft Storm-0558 Incident	550
<i>Hamza Benmiloud, Malek Malkawi</i>	
The URL NextDoor: A Digital Forensic Analysis of Neighborhood Apps	557
<i>Joseph Brown, Abdur Rahman Onik, Ibrahim Baggili</i>	
(SEAL) Sequentially EvolvingAlert Learning for SmartCyber Security	565
<i>Riona. V, R. Hemalatha</i>	
Beyond Charts - Financial Prediction With Language Model & Time Series	571
<i>Sudesh Pawar</i>	

Large-Scale Financial Forecasting Using Advanced GAI-Based Large Language Models and Time Series Analysis	577
<i>Surya Veera Brahmaji Rao Sunnam</i>	
Comprehensive Review and Experimental Study of Holiday-Aware Multimodal Crime Prediction	583
<i>Sapna V. M, Vishruth S. Megur, Vishwanath Bhavimani, Somesh S, Vignesh Madivala, Prasad B Honnavalli</i>	
Big Data-Driven AI Models for Network Anomaly Detection and Cyber Threat Forecasting	589
<i>Amit Kumar Meshram, Vikrant Sikarwar</i>	
Drone Assisted Remote Wellness Monitoring Using RGB Camera	595
<i>Egemen Bora Tuncarslan, Ihsan Yilmaz</i>	
Linear Cryptanalysis of Block Cipher LELBC	601
<i>Yingjie Zhang, Gang Liu</i>	
DarkTraceUI: A Multimodal Framework for Identifying Dark Patterns in Web and Tor Ecosystems	606
<i>Sapna V M, Prakruthi G P, Karthik H Kademani, Keerthana M, Likhith Avinash V, Prasad B. Honnavalli</i>	
Artificial Intelligence-Based Anti-Money Laundering Solutions: Enhancing Detection Accuracy in High-Volume Financial Data	612
<i>Amit Kumar Meshram, Vikrant Sikarwar</i>	
Enhancing Detection of Bloodstain Patterns and Footprint Impressions Using Deep Learning	618
<i>Thangavel Murugan, Maryam Saif Abdulla Saeed Almazrouei, Hind Abdulla Asman Balmur Al Ameri</i> <i>N Nasurudeen Ahamed, Aysha Salem Hamdan Obaid Alkaabi, Priyan Malarvizhi Kumar</i> <i>Shamsa Rashid Salem Balhas Alshamsi, Alia Ali Salem Alwali Almazrouei</i>	
Telegram as a Transformative Criminal Marketplace: Analyzing Identity Theft Dynamics on Surface-Accessible Platforms	624
<i>Manik Kaur, David Maimon, Mario M. Kubek, Anu G. Bourgeois</i>	
An Explainable AI Study of Phishing Detection Model Degradation Across Real-World Events	630
<i>Michael Ivanicki, Brian Robert Callahan</i>	
Unsupervised Baseline Clustering and Incremental Adaptation for IoT Device Traffic Profiling	635
<i>Sean M. Alderman, John D. Hastings</i>	
PALM: Prototype-Aligned Label Manifold Learning for Multi-Label Classification with Partial Annotations	641
<i>Yuqi Song, Xin Zhang</i>	
AdaptIndex: Adaptive Index Selection for IoT Vector Databases	647
<i>Chandrashekhar Medicherla, Chaitanya Kulkarni, Viswanathan Ranganathan, Milan Parikh, Vinay Soni</i>	
An Investigation on the Application of Pareto Principle to Windows Based System Resource Usage	653
<i>Mihai Lazarescu, Sieteng Soh</i>	
TRPO Multi-Agent Active Learning for Explainable DDoS Detection in Healthcare IoMT	659
<i>Omar Farshad Jeelani, Viktoriia M. Korzhuk</i>	
Performance Analysis of Field-Level Encryption on Structured Sensitive Data Using Elliptic Curves	665
<i>Anxhela Baraj, Jonatan Lerga</i>	

Evaluating Security Policy Compliance in Infrastructure as Code Generated by Large Language Models	670
<i>Ryo Hase, Ye Wang, Toshiaki Koike-Akino, Jing Liu, Kieran Parsons, Jumpei Hato</i>	
A Hybrid Graph-Based Analysis Framework for Discovering Relational Fraud Patterns	676
<i>Büşra Demir Sezgin, Hakan Burak Emekli</i>	
AskCMMC.ai for AI-Driven CMMC 2.0 Compliance Automation	682
<i>Hala Strohmier Berry, Aaryan R Londhe, Addur Rahman Khan, Ronit Pawar</i>	
Yolo11s Optimization for Minutiae Detection	690
<i>Ahsan Ul Islam, Wadduwege Shanika Perera, Erasmus Mfodwo, Van Vung Pham</i>	
Stack Buffer Overflow Risk Analysis for PX4-Controlled Commercial UAVs	697
<i>Chris Clark, Hala Strohmier Berry, Kadin DeMesme, Marco Paolo Saavedra, Travis Samatov</i>	
Bounced Check Risk Prediction via Multi-Objective Hyperparameter Optimization: Balancing Macro F1 and Business Uplift	704
<i>Kerem Kaya, Emir Çetin Memiş, Seyit Ertuğrul, Hakan Karamanlı, Erkal Bıyıklıoğlu, Yassine Drias Semen Son-Turan, Nazlı Torağanlı-Karamollaoğlu, Tuna Çakar</i>	
A Comparative Study of Machine Learning Models for Micro-Segment Credit Risk Prediction	709
<i>Kerem Kaya, Emir Çetin Memiş, Seyit Ertuğrul, Hakan Karamanlı, Yassine Drias, Semen Son-Turan Nazlı Torağanlı-Karamollaoğlu, Tuna Çakar</i>	
An LLM-Powered API Testing Framework Based on Structural Similarity Analysis	714
<i>Anıl Sezgin, Tuğberk Kocatekin, Mert Yağcıoğlu</i>	
Evidence-Quality Telemetry for Cloud Incident Response: Detecting Gaps, Drift, and Integrity Failures in Large-Scale Observability Pipelines	720
<i>Chalapathi Koneni, Sanjay Lokula</i>	
Advancing Fire and Smoke Detection in Forensic Surveillance: A Study with Context Aware Augmentation and Optimization	726
<i>Paul N. Isibor, Pamela Kirui, Osayomore O. Aigbogun, Isah Mohammed, Bright Jiwueze, Van Vung Pham</i>	
Event-Driven Agentic SOC (ED-ASOC): Supervisor-Based LLM Framework for Dynamic Incident Response and SOAR Orchestration	733
<i>Enes Özgözler, Asaf Varol, İhsan Tanrıverdi</i>	
Volatile Memory Forensics of Tails OS in a Virtualized Environment	738
<i>Nurettin Senol, Jayden Thai, Semih Cal, Ahmet Aydoğan</i>	
Agentic Framework for Continuous Revenue Governance Across CRM, CPQ, and CLM	745
<i>Sivasai Nadella</i>	
Integrating Generative AI Into Retail Checkout Systems: A Case Study in Cloud and Application Integration	752
<i>Gopalakrishnan Venkatasubbu, Rajgopal Devabhaktuni</i>	
Neuro-Symbolic Graph Autoencoders with Rare Pattern Mining for Provenance-Based Anomaly Detection	758
<i>Asif Tauhid, Sidahmed Benabderrahmane, Mohamad Altrabulsi, Ahamed Foisal, Talal Rahwan</i>	
Personalized Product Recommendation in E-Commerce Using Machine Learning Techniques	764
<i>Navdeep Singh</i>	

Performance Analysis of a Cloud-Native Web Application Deployed on Kubernetes	770
<i>Dharmendra Ahuja</i>	
High Accuracy is Not Enough: Epistemic Bias in Machine Learning Task Formulation	776
<i>Grazia Garzo, Alessandro Palumbo</i>	
Fakespeech: LLM-Driven Semantic Manipulation and Voice Cloning for Realistic Deepfake Speech Benchmarking	782
<i>Alaa Alsaeedi, Amal AlMansour, Amani Jamal</i>	
Gradient-Accelerated Cosmological Inference: A JAX-Based Framework for Differentiable Bayesian Computation in Astrophysics	789
<i>Mayank Jha</i>	
XGBoost-Enhanced Recurrent Hybrid Models for Wearable Inertial Navigation in GNSS-Denied Environments	795
<i>Yash Sinha, Vedant Singh, Tushar Swami, SK Hithasree, Nagalakshmi SR</i>	
Malware Classification on PE Files Using Deep Neural Networks	801
<i>Daniel Vilaça, Luís Ferreira</i>	
Digital Forensics Applications of Electric Network Frequency	808
<i>Fatih Yaman, Ümmühan Özkaynak, Fatih Özkaynak</i>	
Incident-Aware CI/CD Pipelines: Learning from Production Failures to Prevent Certificate Rotation Drift	814
<i>Yogesh S. Thanvi, Lakshmi Vidya Peri, Yogeesh Kunigal Gangaiah</i>	
Porting and Evaluating Return-Oriented Programming Defenses Implemented by the OpenBSD Operating System	820
<i>Jenna Esposito, Aaila Arif, Raul Cortinas, Brian Robert Callahan</i>	
Extending the TMMi Framework for Secure Testing of AI Agents	827
<i>Lakshmi Vidya Peri</i>	
Version-Controlled Decentralized Firmware Integrity Verification With On-Chain Rollback Protection for Cyber-Physical Systems on Ethereum	833
<i>Maruf Farhan, Usman Butt, Madhuki Rajapakshe, Rejwan Bin Sulaiman</i>	
Post-Quantum Cryptography for Web Authentication Protocols: A Systematic Review of OAuth 2.0, OpenID Connect, and SAML Migration	841
<i>Ravindu Dissanayake, Harindu Wijesinghe, Jaith Vindinu, Kulanga Jayasinghe, Kavinga Abeywardena Amila Senarathne</i>	
SafeKid Scan: Early Detection of Digital Addiction in Minors	847
<i>Anjana H.H. H, Y.P. Weerakkodi, Gimhani J.M.K. P, M.A.N. Nethmini, Jenny Krishara Poorna Panduwawala</i>	
QSignature 1.0: A Dynamical Regime Classification Framework for Causal Time Series Data	853
<i>Ahmad Muhammad, Salim Jibrin Danbatta, Muhammad Abubakar Isah, Ibrahim Yahaya Muhammad Sulaiman Sulaiman Ahmad, Abdelrahman Ghozlan</i>	

An Interpretable Multimodal AI Framework for Severity-Aware and Guideline-Aligned Treatment Recommendation in Chronic Spontaneous Urticaria	859
<i>Samidi Jayawickrama, Ramindu Nimes, Thewan Damnidu, Pradicksa Pradeepraj</i>	
<i>Dharshana Kasthurirathna, Samantha Siriwardana</i>	
Romance Scam Reporting and Support: Help-Seeking Timing, Trust, and Escalation	865
<i>LD Herrera</i>	
Governance and Auditability of AI-Driven Retail Decision Pipelines in Cloud-Native Architectures	871
<i>Prithvi raj Veluchamy</i>	
Information Security Web System Based on the ISO 27001 Standard: A Case Study in a Construction Company in Lima	876
<i>Eduardo Giordano Torres Rossi, Rosmery Milagros Pardave Huerta, Ernesto Adolfo Carrera Salas</i>	
Contextual Reinforcement Learning for Linguistic Intent-Gated Access Control in Production AI Systems	882
<i>Karthik Pappu</i>	
Machine Learning-Driven Threat Detection and Response Framework for Modern Cybersecurity Systems	888
<i>Sathesh P. Sivashanmugam</i>	
Ransomware Attacks on AI Systems: a Cross-Domain Threat and Control Analysis	894
<i>Yuvaraj Govindarajulu, Behnaz Karimi</i>	
Predictive Models for Urban Air Quality Management Using AI	901
<i>Dulara Liyanage, Nimasha Vithanage, Imasha Wijewardane, Nimasha Fernando, Dinuka Wijendra</i>	
<i>Thamali Dassanayake</i>	
On Optimal Power Allocation in Downlink Multicarrier NOMA Systems	907
<i>Muhammad Nomani Kabir, Yasser M. Alginahi, Wael Said, Golam Saleh Ahmed Salem</i>	
MorphoNet-Mugil: A Deep Learning-Based Application for Automated Morphometric Measurement of Mugil Cephalus	912
<i>Charlie S. Marzan</i>	
Enhancing Phishing Url Detection with Machine Learning Algorithms	918
<i>Weijie Pang, Ashar Neyaz, Raymond Eichner</i>	
Adversarial Robustness of ML-Based Intrusion Detection Systems	923
<i>Dmitry Sivkov, Viktoriia Korzhuk, Roman Safiullin, Omar Farshad Jeelani, Alisa Vorobeva</i>	
Temporal Behavioral Archetypes of Ransomware in Active Directory Environments	929
<i>Prajna Bhandary, Charles Nicholas</i>	
Exploration of Bottlenecks and Optimizations in Privacy-Preserving Machine Learning Inference	935
<i>Bingyu Liu, Salem Othman, Leonidas Deligiannidis, Robbie McCue</i>	
Cross-Language Transfer Learning for Vulnerability Detection: Directional Asymmetry Between Java and Python	942
<i>Adiba Mahmud, Yasmeen Rawajfih, Fan Wu</i>	
Robust Watermarking for Satellite Imagery: Leveraging Semantically Insignificant Areas	947
<i>Pham Ngok Hung, Aleksey Maksimov, Victor Fedoseev</i>	

A Systematic Study of Security and Privacy in Large Language Models	952
<i>Bingyu Liu</i>	
Trustworthy and Reliable Machine Learning for Healthcare	960
<i>Bingyu Liu</i>	
Detecting Fileless Malware Through Memory Forensics with Recurrent Neural Networks	964
<i>Noah Preston, Ajay Kumara Makanahalli Annaiah</i>	
From Binary Vulnerability Detection to CWE Classification: A Hierarchical Prompting Study	970
<i>Obinna Okeke, Sushant Nepal, Venkat Sai Suman Lamba Karanam, Yan Wu</i>	
BloodTrace: Where Drops Become Decision	976
<i>Dharanidharan Ranganathan, Devkumar Barot, Qian Liu, Oluwasola Mary Adedayo</i>	
Transfer Learning for Malware Detection Using RGB Binary Visualization: A Comparative Study	983
<i>Eva Tuba, Ivona Brajevic, Adis Alihodzic, Ana Trisovic, Milan Tuba</i>	
On Impact of Ensemble Strategies in Tabular Data Regression	989
<i>Ivona Brajevic, Una Tuba, Milan Tuba</i>	
DARKMINE: Deep Learning for Dark Web Threat Intelligence - Anonymous Attack Infrastructure Attribution and Criminal Organization Detection	995
<i>Usha Ratnam Jammula, Naga Sujitha Vummaneni</i>	
AI-Driven Adaptive Training Architecture for Post-Disaster Structural Damage Assessment	1001
<i>Hüseyin Deniz, Vahtettin Cem Baydoğan, Bahar Demirel, Fatih Özkaynak</i>	
Lifecycle-Integrated Security for AI-Cloud Convergence in Cyber-Physical Infrastructure	1007
<i>S M Zia Ur Rashid, Deepa Gurung, Sonam Raj Gupta, Suman Rath</i>	
Beyond NVD: Regional Vulnerability Databases for Global Coverage	1013
<i>Shashank Koganti, Subhasish Mazumdar</i>	
TRADES-Based Defense Against Adversarial Attacks in Medical Image Classification	1019
<i>Kily Jasso, Audrey Tollett, Ira Tuba, Eva Tuba</i>	
Selective Memory Sharing in Multi-Agent LLM Teams via AgentGym-RL	1025
<i>Bhavuk Jain, Gunjan Jain, Hardeo K. Thakur</i>	
Artificial Intelligence-Driven Predictive Models for Identifying Risk Factors of Chronic Diseases	1031
<i>Shaiful Mahmud, Khaleel Khan Mohammed, Vasu Raj Jain, Sarthak Anandkumar Shah</i>	
Enterprise-Grade AI-Driven Text Analytics and Insight Extraction Using Transformer-Based NLP Models	1037
<i>Chandra Prakash Singh</i>	
Pharma Supply Chain Cyber Risk Dashboard: Visualizing Threats and Applying CNSS Controls Across Suppliers, Manufacturers, and Distributors	1043
<i>Pravallika Gummdivelli, Gahangir Hossain</i>	
Securing Clinical Trial Data Vaults: A CIA-Driven Architecture for Confidentiality, Integrity, and Availability	1048
<i>Pardhiv Vasireddy, Yahya Awaad, Gahangir Hossain</i>	

AI for DevSecOps Optimization: Investigating the Role of AI/ML in Predictive Vulnerability Detection During CI/CD Pipeline Stages	1055
<i>Tarun Kalwani</i>	
LLM-Augmented Agentic Consensus Swarms for Autonomous Edge Security	1061
<i>Raju Dandigam, Ravi Teja Thutari, Tejaskumar Vaidya</i>	
Productizing AI-Driven Network Security Systems: Architecture, Trade-Offs, and Product Management Perspectives	1069
<i>Balu Chavan</i>	
Akura: Adaptive Sinhala Learning for Early Childhood Using Gesture, Voice, Emotion and Handwriting	1074
<i>N. W. P. G. T. Mihiran, R. M. D. S. Rathnayake, H. A. D. T. Piyathilaka, N. W. P. G. T. T. Rahul Dinuka Wijendra, Jenny Krishara</i>	
High-Performance Distributed Deep Learning Using Adaptive Parallelism and Dynamic Workload Scheduling	1080
<i>Pavan Kumar Boyapati, Siva Teja Reddy Kandula</i>	
Automating Organizational Cyber Security Policy Compliance Against Industry Standards Using Agentic AI	1086
<i>Rohit Negi, Soumyo V. Chakraborty, Amit Negi, Sandeep K. Shukla</i>	
Data Protection and National Security Implications of Post-Disaster Structural Damage Assessment Systems	1092
<i>Vahtettin Cem Baydoğan, Bahar Demirel, Tuba Demir, Sedat Savaş, Ferhat Uçar, Fatih Özkaynak</i>	
Tamper Detection in CT DICOM Images for Digital Forensics and Clinical Integrity Using Deep Learning	1098
<i>Hala Strohmier Berry, William Carroll, Jessica Brown, Sydney Halupa</i>	
Lean-Driven SAP Production Planning Optimization Using Machine Learning for Inventory and Throughput Efficiency	1105
<i>Mahendrakumar Kalal</i>	
Real-Time Vision-Based Human—Robot Interaction Framework for Low-Cost Embedded Robotic Arms	1111
<i>Wewage Anjana Pruthuvi Dep, Vishimi Embuldeniya</i>	
DASTestBed: An Automated Benchmarking Framework for DAST Scanners with Extensible Ground Truth Modeling	1116
<i>Rand Deeb, Alisa Vorobeva, Omar Farshad Jeelani</i>	
Feature-Equivalence Deduplication and Memoization of HTTP(S) Requests for Web Scanners: Formal Model, Concurrency, and Complexity Bounds	1123
<i>Rand Deeb, Alisa Vorobeva, Omar Farshad Jeelani</i>	
Data-Driven Prediction of Advertising Digital Campaign Effectiveness Using Artificial Intelligence	1129
<i>Abhinay Kumar Reddy Seella</i>	
A Controlled Comparative Study of MongoDB Security Under REST and GraphQL APIs With Proxy-Based Protection	1135
<i>Sapna V. M., Shruti Kumari, Siddhi Jhade, Tejas Gowrish, Ullas Girish, Prasad B Honnavalli</i>	

Performance Analysis of a Multi-Stage Transfer Learning for Brain Disease Classification Using CLAHE-Enhanced 3D-Rendered MRI Images	1141
<i>Isaac Angelo M. Dioses, Jesusimo L. Dioses, Alexander A. Hernandez</i>	
A SWOT Analysis of Mobile Privacy and Security Education for K-12 Students	1147
<i>Tayiba Raheem, Mary Nusrat, Gahangir Hossain</i>	
An RFID-Assisted Machine Learning Approach for Robust Face Recognition	1153
<i>Aminul Islam, Atia Farzana Chowdury, Abdullah Al Mamun, Nur Hossain Bhuiyan</i>	
Automated Extraction of Browser History from Computer Hard Disks	1160
<i>Sakar Joshi, Sankardas Roy</i>	
Devsecops-Driven Security Controls for ERP Release Pipelines	1166
<i>Yogesh Kunigal Gangaiah, Karthik Pappu, Yogesh S. Thanvi</i>	
Comparative Study of Symbolic Execution Tools Applied to Vulnerability Detection	1172
<i>André Cardoso, Óscar Ribeiro, Nuno Lopes</i>	
AI-Driven Malware Defense: Transformer Model for Real-Time Detection and Threat Analysis	1178
<i>Viktoria Meskova, Natalia Valencia, Gustavo A. Chaparro-Baquero, Alexander Perez-Pons</i>	
Evaluating the Reliability of Generative Ai in Software Engineering Refactoring Tasks	1185
<i>Zhala Sarkawt Othman, Murat Karabatak</i>	
Shortcutprobe: Identifying Backdoor Samples Via Internal Stability Analysis	1190
<i>Mahaveer Prasad, Ajit Kumar Yadav, Rajeev Kumar, Victor Fedoseev</i>	
An Investigation of the Relationship Between Preservice Teachers' Artificial Intelligence Awareness and Anxiety Levels	1196
<i>Ahsen Aslantaş, Songül Karabatak, Murat Karabatak</i>	
Deep Learning-Based Classification of Cutting Tool Wear in Dry Turning of Ti-6Al-4V Using Thermography	1201
<i>Büşra Tan Saatçıl, Mustafa Ulaş, Turan Gürgeç, Engin Ünal</i>	
Technical Framework for Combating Deepfake Identity Fraud in E-Government Services	1207
<i>Elie Hanna, Ezzeddine Abou Zahr, Khouloud Samrouth, Nader Bakir</i>	