

2026 IEEE 5th International Conference on AI in Cybersecurity (ICAIC 2026)

**Houston, Texas, USA
18-20 February 2026**

Pages 1-651



**IEEE Catalog Number: CFP26BD1-POD
ISBN: 978-1-6654-7762-8**

**Copyright © 2026 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:	CFP26BD1-POD
ISBN (Print-On-Demand):	978-1-6654-7762-8
ISBN (Online):	978-1-6654-7761-1

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

Architecting Agentic AI Systems with Multimodal Reasoning for Scalable Visual Pattern Recognition	1
<i>Linga Reddy Alva, Hari Shanker Reddy Resu</i>	
CodeGraph- Malware Detection via Control Flow Graph Embeddings and Graph Neural Networks	7
<i>Chandrashekhara Medicherla, Chaitanya Kulkarni, Rajesh Purushothaman, Rakesh Keshava, Arun Kumar, Nandagopal Sheshagara</i>	
Supply Chain with Sixth Sense Agentic AI: A Proactive Intelligence Framework for Autonomous Planning.....	13
<i>Venkatesh Prabu Parthasarathy, Madhusudan Sharma Vadigicherla</i>	
Identity-Spoofing Prompt Injection: Empirical Analysis of Instruction Leakage in Custom GPTs	20
<i>Abid Ahmad, Fayzuddin Topu, Joyana Islam, Amit Banwari Gupta, Md. Maruf Hassan</i>	
AI-Driven Frontend Cybersecurity for Swift and ReactJS Applications Using Public Phishing and Malicious Web Datasets	27
<i>Mykola Savenko, Ilia Sedoshkin</i>	
From Science to Production: A Systematic Framework for Operationalizing and Governing Machine Learning Models.....	35
<i>Vamshi Krishna Pamula</i>	
AI-Driven Cybersecurity for SCADA-Integrated Microgrids: A Real-Time Detection Framework.....	39
<i>Alaa Saleem Athamnih, Samir Abood, Mohamed Chouikha, Annamalai Annamalai, Colby Woodard, Huda Al-zuhairi</i>	
Generative Temporal Diffusion Models for Early Prediction of Cloud Service Degradation	45
<i>Sabitha Muppuri</i>	
Codebase Aware Generative Agents for the SDLC: Automating Documentation, Dependency Analysis and Test Generation	52
<i>Vatsal Kishorbhai Mavani</i>	
Interpretable Generative AI for Predictive Project Risk and Success Analytics.....	56
<i>Madhusudan Nagaraja, Abhishek Jain, Renuka Yallappa Hosamani</i>	
Combined Tempered MRG32k3a: A High-Quality and Reproducible Pseudo-Random Number Generator for AI in Cybersecurity	62
<i>Hussein Alzoubi</i>	
Quantifying Risk Reduction: AI-Driven Model for Automating Access Certification and Segregation of Duties (SOD) Controls.....	66
<i>Sunnykumar Kamani</i>	
Early Detection and Prediction of Depression Based on Data-Driven Machine Learning Techniques in Mental Healthcare	71
<i>Sanjoy Mukherjee</i>	
Integrating AI into DevSecOps Pipelines for Secure Cloud Microservices Management.....	77
<i>Atish Kumar Dash</i>	

GraphAE: Plant-informed Graph Autoencoder for ICS Anomaly Detection with SHAP-based Explanations	84
<i>Vahid Heydari, Kofi Nyarko</i>	
FraudSentinel: Federated Multi-Agent Reinforcement Learning for Privacy-Preserving Cross-Marketplace Fraud Detection in Distributed E-Commerce Ecosystems	89
<i>Tejas Pravinbhai Patel, Chaitanya Kulkarni, Deepak Kole, Milan Parikh, Rakesh Keshava, Rajesh Purushothaman</i>	
Designing Effective Quantum Generators: A Comparative Study of Variational Ansätze in Hybrid QGANs.....	95
<i>Sarvapriya Tripathi, Aakarsh Etar, Jayesh Soni, Himanshu Upadhyay</i>	
Predictive Green FinOps: Joint Optimization of Cost, Carbon, and Reliability in AI-Intensive Clouds.....	101
<i>Venkata Thej Deep Jakkaraju, V. Jayaprakasan</i>	
Quad-Stream Deepfake Detection: Combining Spatial and Frequency Domain Analysis for Robust Video Authentication	107
<i>Vaishnav Anand, Ivan Felipe Rodriguez</i>	
The Medallion Architecture in Practice: A Framework for Building Scalable and Governed Data Lakehouses on Microsoft Fabric	116
<i>Vamshi Krishna Pamula</i>	
Securing the LLM Supply Chain: Analyzing Threats and Mitigation Strategies	121
<i>Atish Kumar Dash</i>	
Real-Time Multi-Source Threat Intelligence Fusion Using Large Language Models.....	128
<i>Abdullah Al Siam, Moutaz Alazab, Areej Obeidat, Nuruzzaman Faruqui, Somaya Al-Maadeed</i>	
A Review of User Account Anomaly Detection and Insider Threat Detection Techniques.....	134
<i>Joe Childress, Manki Min</i>	
Integrating AI and Cloud to Advance Scalable, Secure, and Automated Information Management in Enterprises.....	139
<i>Shiva Krishna Kodithyala, Hari Shanker Reddy Resu</i>	
Automating Multi-Cloud Deployments at Scale Using an Advanced GitOps Framework.....	144
<i>Vishwa Lakhnakiya</i>	
Reinforcement Learning Integrated Agentic RAG for Software Test Cases Authoring	149
<i>Mohanakrishnan Hariharan</i>	
AI Driven Multi Cloud Strategies for Financial Services: Ensuring High Availability with AWS and Kubernetes.....	154
<i>Jigar Mahendrabhai Solanki</i>	
Artificial Intelligence (AI)-Driven Network Traffic Anomaly Detection for IT Infrastructure Security.....	159
<i>Dileep Jain, Sharad Jain</i>	
ZT-ICAS: A Zero-Trust Integrity-Constrained Framework for Agentic Vulnerability Scanning	165
<i>Jothsna Praveena Pendyala, Sumeet Jeswani</i>	

AI-Driven Claims Adjudication: Optimizing Healthcare Systems with Machine Learning and Deep Neural Networks.....	172
<i>Damodhara Reddy Palavali, Suneetha Pothireddy, Dinesh Kumar Elumalai, Madhusudan Nagaraja</i>	
Explainable Machine Learning for Malware Detection: A SHAP-Based LightGBM Framework.....	178
<i>Abdullah Al Siam, Hazem Abu-Adaiq, Mahdee Nafis, Ferdous Anwar Anik, Sabbir Mahmud, Md Maruf Hassan</i>	
Securing 5G/6G Networks: Handover, Slicing, and QoS Security Issues	184
<i>Hritesh Yadav, Varun Singh, Kshitij Sharma, Suyash Karmarkar, Akhilesh Keshap</i>	
A Survey on Machine Learning Applications for Operating System Fingerprinting.....	190
<i>Siri Siqveland, Alexandra Newcomb, Omar Ochoa</i>	
AI-Optimized VLSI Architecture for Energy-Efficient and Sustainable IoT Systems	197
<i>Shujaatali Badami, Anshul Sharma, Bhaskar Reddy, Shailesh Kadam, Biky Chouhan, Brijeena Rana</i>	
TrustGraph: Federated Graph Neural Networks for Cross-Platform Trust and Fraud Propagation Analysis	204
<i>Tejas Pravinbhai Patel, Arun Kumar, Madhushree Kumari, Rajesh Purushothaman, Rakesh Keshava, Milan Parikh</i>	
Zero-Shot Tokenizer Transfer for Targeted Attacks on Retrieval-Augmented Generation.....	210
<i>Edward French, Samyam Aryal, Aman Singh, Komal Subhash More, Joe Hammond, Mark Spanier</i>	
Breaking the Monolith: A Data-First Strategy for Enterprise Microservices Migration with Measured Improvements in Scalability and Resilience	216
<i>Venkaiah Chirumavilla</i>	
Quantum-Resilient Secure Framework for Agentic LLM Workflows in E-Commerce and FinTech Systems.....	222
<i>Phaneendra Vayu Kumar Yerra, Naga Subrahmanyam Cherukapalle</i>	
AI-Guided Adaptive Compression for Secure and Efficient Web Resource Delivery.....	229
<i>Kateryna Babii, Oleh Polishchuk</i>	
Evaluating Modern Software Design Trends for Efficient and Maintainable Application Development	233
<i>Ashish Pokhrel</i>	
Scalable Graph-Based Detection of Fraud Rings in Large-Scale Networks.....	239
<i>Xiantian Zhou, Qixin Deng, Aobo Jin, Hardik Gohel</i>	
Advancing Cybersecurity in Critical Infrastructure Systems via Machine Learning-Based Threat Detection and Mitigation.....	248
<i>Siva Teja Reddy Kandula, Pavan Kumar Boyapati</i>	
A Hybrid Methodology for SAP Implementations: Blending ASAP with Agile Principles for Enhanced Flexibility and Stakeholder Engagement	255
<i>Harsh Patel</i>	
A Secure and Scalable Cloud-Based Banking Service Model Leveraging AI and Advanced Cyber Security.....	261
<i>Sreenivasulu Gajula, Madhuri Margam</i>	

HCT-Net: A Hybrid Convolutional and Transformer Based Network for Corrosion Detection in Industrial Images	266
<i>Mohini Gohel, Aparna Aravelli</i>	
Novel Textual Data Cleaning Techniques for Cybersecurity Recommendation Extraction and Prioritization using Local LLMs	272
<i>Aisvarya Adeseye, Jouni Isoaho, Seppo Virtanen, Mohammad Tahir</i>	
TransCall: A Transformer-Driven Framework for Zero-Day Malware Detection Using System Call Sequences	278
<i>Abdullah Al Siam, Moutaz Alazab, Areej Obeidat, Nuruzzaman Faruqui, Somaya Al-Maadeed</i>	
Multi-Layered Defense Proxy for Home Assistant utilizing Large Language Models.....	284
<i>Faran Yazdani, Stephen Antezana, Mohamed Gebril, Sherif Abdelhamid</i>	
Machine Learning-Enabled Classification of Diabetes Using Clinical via Lifestyle Health Data	290
<i>Sanjoy Mukherjee</i>	
AI-Driven DDoS Detection for Network Security: A Performance Analysis of Machine-Deep Learning Methods on Network Traffic Data.....	296
<i>Manoj Kumar, Maunik K Shah</i>	
A Framework on Advancing Cybersecurity Education via Quantum Machine Learning.....	302
<i>Celestina D Kolog, Xian Mallory, Jie Yan, Hongmei Chi</i>	
ChatXplain: Interpretable Explanations for Intelligent Assistants via Modular Rationale and Saliency	311
<i>Satya Karteek Gudipati, Naveen Anand Mishra, Akbar Mohammed, Sambasiva Rao Akkiseti, Gopikanth Ankam, Sateeshkumar Ponugoti</i>	
Resource Allocation in 6G Networks: A Comprehensive Review of Machine Learning Approaches	319
<i>Devanand Patil, Joydev Ghosh, Bishwajeet Kumar Pandey</i>	
AI-Assisted Detection of Malicious Changes in Infrastructure-as-Code for Secure DevOps	325
<i>Shalini Sudarsan, Manan Agrawal, Ankita Banerjee</i>	
Integrating Customer Data Platforms (CDPs) with Experimentation Tools: A Framework for Optimizing Customer Journey Revenue.....	331
<i>Gopi Krishna Pamula</i>	
Intelligent Repair Bots for Power BI: An Agentic Automation Approach.....	335
<i>Mohith Reddy Patlolla</i>	
Interval-Based Estimation of Generalization Accuracy in Supervised Learning via Confusion Matrix Resampling and Bayesian Inference.....	340
<i>Amir Liron, Francis A Mendez Mediavilla, Jesus Jimenez, Abhimanyu Sharotry</i>	
Secure Agent-Based Architectures for Decentralized AI Identity Management: The DAIS Framework.....	349
<i>Viswapriyan Ragupathy</i>	
AI-Driven Prediction of Flexural Properties in Kevlar/Carbon/Glass Fiber Hybrid Composites Using Random Forest Regression	355
<i>Sathish Pandurangan, Syed Mudassir, John C.Chris Becking, Prasanna Ranjith Christodoss, Mithun V Kulkarni, Ahmed Shammass</i>	

Unknown Threat Detection using AI, ML and DL methods.....	363
<i>Manjunath Venkatram</i>	
Enterprise-Grade Security for the Model Context Protocol (MCP): Frameworks and Mitigation Strategies	369
<i>Vineeth Sai Narajala, Idan Habler</i>	
Swarm Optimization Algorithm-Enhanced Clustering Techniques for Reliable Wireless Sensor Networks Communication.....	377
<i>Mitesh Patel, Uday Korat</i>	
Neuromorphic Computing Architectures for Synthetic-Data AI in IT Infrastructure	383
<i>Shilpi Mittal, Ankit Gupta</i>	
Optimizing AI-Driven Mobile Applications on iOS: A Comparative Analysis of Core ML and TensorFlow Lite for Cross-Platform Performance	386
<i>Rutul Desai</i>	
HRIT: A Human-Readable Framework for Phishing URL Detection using Large Language Models	391
<i>Tanya Yadav, Mohammad Masum</i>	
LLM-Based Decision Making Framework for Autonomous Drone Navigation	397
<i>Mirza Aarish Baig, Brad Alvarez, Richard Lage, Jayesh Soni, Himanshi Upadhyay</i>	
AI-Driven Detection of AI-Generated Cyber Attacks: A Framework for Defending Against Generative Adversarial Threats	402
<i>Tanvir H. Sardar, Bishwajeet Pandey, Laura Aldasheva</i>	
Next-Generation Digital Twin Analytics in Smart Manufacturing using Cross-Layered Edge Cloud Deep Learning	407
<i>Saisuman Singamsetty, Sudheer Singamsetty, S Satyanarayana, Puranam Revanth Kumar</i>	
Identity Governance in DevSecOps: Automated Access Reviews for CI/CD Pipelines.....	413
<i>Sunnykumar Kamani</i>	
Adaptive Loyalty Systems: A Reinforcement Learning Framework for Dynamic and Context-Aware Benefit Allocation	418
<i>Tarun Kalwani, Balakumaran Sugumar</i>	
DeepNetDetect: A Deep Learning-Based Approach for Early Anomaly Detection in Network Traffic.....	424
<i>Henry P Cyril</i>	
Toward Context-Aware Alert Classification in Security Operations Centers Using LLMs.....	430
<i>Jonathan Roy, Elhadj Abdourahmane Balde</i>	
Optimizing Customer Engagement through IoT Data Integration in CRM Ecosystems	440
<i>Sathish Kumar Velayudam</i>	
DevSecOps-Driven Security Integration in the Software Development Lifecycle Using CI/CD Pipelines	446
<i>Henry P Cyril, Shiva Kumara</i>	
Enhancing Intrusion Detection with Image-Based CNN and CTGAN Synthetic Oversampling.....	452
<i>Leo Martinez, Md Habibur Rahman, Avdesh Mishra, Mais Nijim, Ayush Goyal, David Hicks</i>	

Age-Differentiated Pathways to Privacy Protection in Smart Voice Assistants: A Multigroup PLS-SEM Study of Youth.....	458
<i>Yulia Bobkova, Molly Campbell, Trevor De Clark, Ajay Kumar Shrestha</i>	
Semantic Mastery: Enhancing LLMs with Advanced Natural Language Understanding	466
<i>Mohanakrishnan Hariharan</i>	
Multi-Layered Security Framework for Financial AI Solutions - PISA	473
<i>Aruun K. Kumar, George Belsian, Santosh Srinivasan, Giridhar Shyam Sankararaman</i>	
Causal-Contrastive Graph Neural Networks for Robust, Explainable Multi-Modal Intrusion Detection	479
<i>Sangharsh Agarwal</i>	
Evaluating Jailbreak Vulnerabilities in LLMs: A Taxonomy and Comparative Analysis in Romance Fraud Scenarios	485
<i>Yohn Jairo Parra, Hongmei Chi, Richard A. Alo, Vinicius Lima</i>	
Forecasting and Overcommit Pipelines for Cloud Storage: A Model for Persistent Disk Capacity Management	491
<i>Hareendra Sura</i>	
AI-Driven Quantum Cryptography: Machine Learning for Robust QKD, Secure Operations, and Quantum-Safe Integration	495
<i>Ankit Gupta, Shilpi Mittal</i>	
Secure and Compliant AI/ML-Based KYC: A Cybersecurity-Aware Architecture for Regulatory Identity Verification.....	500
<i>Varun Pandey</i>	
Integrating Price Elasticity and Reinforcement Learning: A Data-Driven Framework for Strategic E-commerce Pricing	506
<i>Dilip Patel</i>	
Architectural Resilience in AI-Driven Decision Systems under Adversarial Conditions.....	512
<i>Viswapriyan Ragupathy</i>	
Bridging the Black Box: Explainable Anomaly Detection for Critical Infrastructure Systems.....	518
<i>John DeLeon, William Mitchell, Shane Waldrop, Serena Reese, Tatum Beaugh, Amiran Fields, Erdogan Dogdu, Roya Choupani</i>	
Privacy-Driven Cloud AI: Federated Learning and Zero-Trust for Secure Multi-Domain Collaboration	527
<i>Prashanthi Matam, Akshay Mittal, Karthik Pappu, VasanthRao Jadav</i>	
A Self-Adaptive Red Teaming Framework for Vulnerability Profiling with Dynamic Attack Graphs and Retrieval Augmented Generation.....	535
<i>Jothisna Praveena Pendyala, Sundeep Bobba, Ali Azghar Hussain Syed Abbas</i>	
Machine Learning Integration in Loan Decision Systems: Enhancing Kafka-Based Workflows with Predictive Analytics.....	542
<i>Jigar Mahendrabhai Solanki</i>	
Strategic Unification: How Blazor is Redefining Enterprise Web & AI Stack.....	546
<i>Venkaiah Chirumavilla</i>	

Assessing Agile Frameworks for Software Development Efficiency Industry Insights and Implementation with Jira Atlassian Agile Tools	552
<i>Ravi Sankar Susarla</i>	
Agent Name Service (ANS): A Universal Directory for Secure AI Agent Discovery and Interoperability	558
<i>Ken Huang, Vineeth Sai Narajala, Idan Habler, Akram Sheriff</i>	
Anomaly Detection in Financial Payment Transactions Using Efficient Data-Driven Machine Learning Techniques.....	567
<i>Sandeep Shivam, Tejas Pravinbhai Patel, Amit Kumar Padhy, Chaitanya Kulkarni, Chandrashekhhar Medicherla, Vinay Soni</i>	
Agentic Commerce: A Comprehensive Analysis of Cybersecurity Risks, Privacy Challenges, and Trust Mechanisms in Autonomous AI-Driven Marketplaces	573
<i>Niranjan Pachaiyappan</i>	
Intelligent Test Data Automation: A Python-Based Framework for Deterministic and Scalable Software Testing	579
<i>Datta Snehith Dupakuntla Naga</i>	
RAGSec: Retrieval-Augmented Generation for Cybersecurity Threat Intelligence in Enterprise Networks	584
<i>Shravya Bussari, Prateek Punj, Gayathri Balakumar</i>	
Non-Intrusive Machine Learning-Based Anomaly Detection for Heterogeneous Embedded Platforms	590
<i>Pranav Gangwani, Alexander Perez-Pons, Himanshu Upadhyay</i>	
Secure Prompt Engineering Patterns for Cloud LLM Agents	597
<i>Shalini Sudarsan, Advait Patel, Charit Upadhyay, Vaishnavi Gudur, Prashanthi Matam</i>	
TrustNet: A Hybrid Machine Learning and LLM-Based Multi-Agent System for Scam Website Detection	603
<i>Sherif Abdelhamid, James Bangura, Katelyn Redlinger, Gunnar Romsland</i>	
Explainable AI for Cloud Intrusion Detection: A User Study of SHAP and LIME in AWS GuardDuty.....	609
<i>Humberto Goncalves, Zakaria Alomari</i>	
A Dual-task Prediction Model for Starlink Maritime Performance.....	617
<i>Richard Li, Md Muntasir Hossain, Xingya Liu, Ruhai Wang</i>	
Lanyard Policy Tracker: A Secure, Privacy-Aware Student Compliance System for K–12 Environments.....	622
<i>Curtis Faughnan, Xiantian Zhou, Aobo Jin, Hardik Gohel, Qixin Deng</i>	
AI-Based Cross-Layer Vulnerability Management for Cloud-Native Systems	630
<i>Oleh Polishchuk, Kateryna Babii</i>	
Federated Transformer Model for Water Contamination Detection in Distributed Monitoring Systems.....	633
<i>Raja Kumar, Jayesh Soni, Himanshu Upadhyay</i>	
Benchmarking Container Orchestration Platforms: A Comparative Analysis of Kubernetes and AWS ECS for Stateful Microservices.....	639
<i>Santosh Kumar Kotakonda</i>	

An Empirical Evaluation of Deep Neural Networks as Hash-Like Mappings Under Digital Signature Threat Models	644
<i>Juan Ortiz Couder, Lynn Vonderhaar, Omar Ochoa</i>	
Client Side AI Based Intent Verification for Defending Against CSRF Attacks in Modern Web Applications.....	652
<i>Kateryna Savenko, Kateryna Babii</i>	
Detecting and Adapting to Normality Shifts in Learning-Based Security Anomaly Detection.....	657
<i>Gaurav Dwivedi, Alexander Perez-Pons</i>	
An Explainable Machine Learning Framework for Predicting Software Defects in Large-Scale Software Systems	666
<i>Srikanth Kavuri</i>	
Machine Learning-Based Fault Prediction in Large- Scale Distributed Systems.....	672
<i>Amit Kumar Padhy, Tejas Pravinbhai Patel, Vinay Soni, Sandeep Shivam, Gajendra Babu Thokala, Bharadwaj Vulugundam</i>	
A Secure Biometric Authentication Framework for iOS with Cross-Platform Extensions: Addressing OS-Level Vulnerabilities and Enhancing Real-Time Protection	678
<i>Rutul Desai</i>	
Software Engineering Challenges in the Deployment of Generative AI Models at Scale	683
<i>Venkata Nagendra Satyam, Braja Gopal Mahapatra, Devisharan Mishra</i>	
A Domain Shift Evaluation Protocol for Fake Satellite Image Detection: CNN Superiority and the Enhanced Model Paradox.....	689
<i>Vaishnav Anand, Ivan Felipe Rodriguez</i>	
AgentSOC: A Multi-Layer Agentic AI Framework for Security Operations Automation.....	697
<i>Joyjit Roy, Samaresh Kumar Singh</i>	
Enclave Driven Tokenization: Reducing PCI DSS Scope in Cloud Native Checkout Systems	704
<i>Rajgopal Devabhaktuni, Gopalakrishnan Venkatasubbu</i>	
Prompt Engineering vs Context Engineering: A Strategic Framework for Insurance AI Applications	710
<i>Rakesh More</i>	
Jailbreaking Large Language Models: Techniques, Trends, Defenses, and Open Challenges	715
<i>Vaishali Vinay</i>	
Integrating Deep Learning with Power BI Admin APIs for Intelligent Data Governance	723
<i>Mohith Reddy Patlolla</i>	
Reverse Entropy Spiral Deep Neural Steganography for Secure Medical Ultrasonogram Videos.....	729
<i>Sheikh Thanbir Alam, R. Badlishah Ahmad, Md. Maruf Hassan, Ku Nurul Fazira Ku Azir, Abubokor Hanip</i>	
Multilingual Image-to-Speech Conversion: Leveraging OCR and Language Translation for Enhanced Accessibility.....	735
<i>Komaldeep Singh, Harkaran Singh, Aakash Rampal</i>	
CityCopilot-X: A Real-Time Explainability Panel for Retrieval-Augmented Generation (RAG).....	740
<i>Satya Karteek Gudipati, Naveen Anand Mishra, Gopikanth Ankam, Sambasiva Rao Akkiseti, Akbar Mohammed, Sateeshkumar Ponugoti</i>	

LLM-Powered Autonomous Security Agents for Next-Generation Cyber Defence.....	749
<i>Tanvir H. Sardar, Bishwajeet Pandey, Laura Aldasheva</i>	
Heart Disease Prediction Using Feature Reconstruction and Hybrid Deep Learning	754
<i>Saba Shamsheer, Sandeep Thota, Hari Suresh Babu, Narendra Chennupati, Shivakrishna Deepak Veeravalli, Manisha Guduri</i>	
Packing Induced Bias in Deep Learning Malware Classifiers: A Systematic Experimental Study	761
<i>Jeevana Swaroop Kalapala, Lan Zhang</i>	
Hybrid Transformer and XGBoost Model for Federated IoT Intrusion Detection	767
<i>Harish Namasivayam Muthuswamy, Madhu Siddharth Suthagar, Velu Natarajan</i>	
Phishing URL Detection Using RNN – LSTM Models for Safer Web Browsing	773
<i>Maitha Falah Alsammak, Roudha Zuhair Bin Redha, Mohamed Basel Almourad</i>	
From UIKit to SwiftUI: A Quantitative Analysis of Migration Strategies for Large-Scale Financial Applications.....	779
<i>Ranjith Kumar Vanaparthi</i>	
Beyond Single-Hop: Link Prediction Through Multi-Hop Reasoning in Malware Knowledge Graphs	784
<i>Kibrom Bahlibi, Hoang Long Nguyen, Erdogan Dogdu, Roya Choupani, William Mitchell</i>	
AI-Driven experimentation for user experience: An Architectural Blueprint for Self-Optimizing iOS Experiences at Enterprise Scale.....	794
<i>Snehal Mehta</i>	
AI-Driven Data Architecture: Building Intelligent Analytics Platforms with Azure and Python.....	800
<i>Suresh Pairu Subramanyam</i>	
Graphene: Leveraging Transformers with Control Flow Modalities for Malware Detection.....	807
<i>Andrew Wheeler, Kshitiz Aryal, Maanak Gupta</i>	
Privacy-Preserving Federated Learning for Multi-Tenant CRM Systems	815
<i>Nidhi Sharma</i>	
Agentic AI Integration for Process Automation in MSMEs	821
<i>Venkatesh Prabu Parthasarathy</i>	
SC-GAN: A GAN-Based Data Augmentation Approach for Stablecoin Fraud Detection on Imbalanced Transaction Data	827
<i>Mohan Sankaran, Nagaraju Jooluri, Srimaan Yarram, Balasundaram Subbusundaram, Balaji Sundareshan</i>	
Accelerating AI Maturity: A Framework for Reducing Development Lifecycles and Increasing Predictive Accuracy.....	833
<i>Gopi Krishna Pamula</i>	
Digital Precognition: Teaching Transformers to Map Cyber Threats Before Analysts Can	838
<i>Shane Waldrop, Erdogan Dogdu, Roya Choupani, William Mitchell</i>	
Confidential and Attack-Resilient Edge LLM Serving for Multilingual Chatbots	849
<i>Satya Karteek Gudipati, Naveen Anand Mishra, Akbar Mohammed, Sambasiva Rao Akkiseti, Gopikanth Ankam, Sateeshkumar Ponugoti</i>	

The Evolution of Agentic AI in Cybersecurity: From Single LLM Reasoners to Multi-Agent Systems and Autonomous Pipelines	858
<i>Vaishali Vinay</i>	
Enhancing Movie Recommendation Systems Through Explainable Machine Learning Models in the Entertainment Industry	866
<i>Hariharan Velu</i>	
Semantic Chunking and Consensus Filtering for Structured Extraction of Cyber Threat Intelligence	872
<i>Shane Waldrop, Erdogan Dogdu, Roya Choupani, William Mitchell, Vitaly Andrejeus, Sawyer Cawthon</i>	
SARS-CoV-2 Classification Using Classical vs. Quantum Machine Learning: A Performance Comparison of SVM, QSVM, and Pegasos.....	883
<i>Sthefanie J. G. Passo, Muntakim Haque, Vishal H. Kothavade, John J. Prevost</i>	
A GenAI-Powered Cybersecurity Mesh for Real-Time Risk Detection in Digital Payments	892
<i>Utham Kumar Anugula, Vijayanand Ananthanarayanan</i>	
Iterative Verification and Batch Processing for Enhancing Accuracy and Confidence Computation in LLM-Based Phishing Email Detection.....	898
<i>Aisvarya Adeseye, Jouni Isoaho</i>	
Security Challenges and Attack Vectors in Modern Steganography.....	905
<i>Sheikh Thanbir Alam, R. Badlishah Ahmad, Md. Maruf Hassan, Ku Nurul Fazira Ku Azir, Amit Banwari Gupta</i>	
Application of Federated Learning to Semantic Segmentation of Aerial Images.....	911
<i>Yong-Lin Kuo, Ying-Wei Chuang</i>	
The Architect of Advantage: How Robust Data Curation and Edge-Case Analysis Provide a Disproportionate Market Edge	917
<i>Rupam Priya</i>	
Enhancing Safety and Performance in Intelligent Vehicular Networks Using Edge-Based Explainable AI Models.....	922
<i>Anshul Sharma, Sravani Lingam, Gayathri Balakumar, Biky Chouhan, Milankumar Rana</i>	
Toward Deployable Disinformation Defense: Benchmarking Lightweight Transformers on FakeNewsNet	928
<i>Humberto Goncalves, Kossi Sam Affambi, Zakaria Alomari</i>	
Leveraging Generative AI And Reinforcement Learning For Autonomous Cyber Threat Mitigation	936
<i>Vaishnavi Gudur, Shiva Kumar Ramavath</i>	
An Autonomous Governance Framework for Generative AI: Real-Time PII Redaction and Compliance in LLM-Driven Data Pipelines	942
<i>Vatsal Kishorbhai Mavani</i>	
GXMalDetect: A Hybrid GA–XGBoost Architecture for Malware Detection Using Static Image Features	946
<i>Abdul Kareem Uddin Mohd, Md Habibur Rahman, Md Wahidur Rahman, Avdesh Mishra, Tarek Mahmud, Maleq Khan</i>	
Optimizing Production Variance and Yield Reporting through Cross-Modular Integration in SAP S/4HANA	952
<i>Harsh Patel</i>	

Harnessing Natural Language Processing (NLP) and Generative AI Techniques for Social Media Sentiment Analysis with Text Classification	956
<i>Bhulakshmi Makkena</i>	
DFT AI: Machine Learning-Guided Test Point Insertion for Pre-Silicon Debug and Post-Silicon Diagnosis in Complex VLSI Systems	962
<i>Deepika Bhatia</i>	
DevOps and CI/CD Maturity in Large-Scale Organizations: A SonarQube and Jenkins Approach.....	968
<i>Suresh Pairu Subramanyam</i>	
Scalable Data Governance Through Engineering-Driven Quality and Consistency Control	975
<i>Gopi Krishna Pamula</i>	
Triangulating Digital Forensics to Detect Friendly Fraud and Abuse at Scale: A Cloud-Native, Agentic AI Framework.....	980
<i>Sabarinathan Govindaraj, Karthik Mahalingam, Velu Natarajan</i>	
LightGBM-Based Multi-Class Botnet Detection Framework for IoT Networks	986
<i>Vidhubala J, Kayalvizhi R</i>	
Hybrid Intelligence Endpoint Defense (HIED): A Data-Fusion Approach for Proactive Malware Detection	992
<i>Michal Jaworski, Bahareh Pahlevanzadeh</i>	
Unified AI Framework for Real-Time Customer Churn Prediction Using Behavioral and Event-Log Anomaly Signals	1000
<i>Jyoti Kunal Shah, Nixalkumar Patel, Darsana Usha Devi, Mahendra Babu Iragala, Ashok Kumar Kunkala, Biky Chouhan</i>	
Real-World Intrusion-Aware Zero Trust Architecture: An AI-Driven ASPM Framework Using CICIDS-2017 Network Attack Traffic.....	1007
<i>Sreenivasulu Gajula, Subhash Bondhala, Madhuri Margam</i>	
AI-Based Cybersecurity in Healthcare: A Data-Driven, Governance-Aware Framework for Secure Clinical Systems	1014
<i>Rajani Kant, Ramachander Rao Thallada, Bishwajeet Pandey, Palak Srivastava</i>	
Enhancing Breast Cancer Diagnosis Using Lightweight Deep Learning Models	1019
<i>Jordan Mozebo, Xiaohong Yuan, Madhuri Siddula, Olusola Odeyomi</i>	
HopeBot: An AI-Powered Mental Health Chatbot Built to Support College Students.....	1026
<i>Abikrit Gautam, Prasanthi Sreekumari</i>	
Reengineering Cybersecurity Processes with Generative AI: From Automation to Strategic Alignment.....	1031
<i>Mehrdad S. Sharbaf</i>	
Automated Validation and Repair of Knowledge Graph Triples for Cyber Threat Intelligence.....	1035
<i>Vitaly Andrejeus, William Mitchell, Sawyer Cawthon, Jesse Sullins, Erdogan Dogdu, Roya Choupani</i>	
Improving Temporal Ordering with External Data.....	1042
<i>Rahul Cherekar</i>	
Resource Allocation of IoT-Based Edge Computing in Smart Cities	1048
<i>Mona Safar Mobark, Abdullah Alqahtani, Naseema Shaik</i>	

A Comprehensive Assessment Tool for Prompt Injection Attacks in Large Language Models (LLMs)	1056
<i>Ailene Dao, Richard VanGorder, Mohamed Gebril, Sherif Abdelhamid</i>	
Comparative Insights: A Multigroup Analysis of Privacy Management Across Youths, Parents, Educators, and AI Professionals in AI Applications	1065
<i>Molly Campbell, Yulia Bobkova, Ajay Kumar Shrestha</i>	
A Cloud-Native Framework for the Petabyte-Scale Purge of Regulated Data: Achieving Compliance and Performance in the Financial Domain	1073
<i>Santosh Kumar Kotakonda</i>	
A Systematic Security Analysis of Model Context Protocol: Vulnerabilities, Exploits, and Mitigations.....	1078
<i>Theophilus Siameh, Abigail Akosua Addobea, Chun-Hung Liu, Eric Kudjoe Fiah</i>	
Proactive Discrepancy Detection at Scale: A Continuous Validation Framework for Distributed Data Systems	1086
<i>Hareendra Sura</i>	
LIARS: Low-Information Area Recognition for Steganography	1090
<i>Claudia Larramendi-Ferras, Alexander Perez-Pons, Gustavo Chaparro-Baquero</i>	
Leveraging Artificial Intelligence to Predict Unfunded Loans in Peer-to-Peer Lending Platforms	1096
<i>Mousumi Munmun, Queen E. Booker</i>	
Adaptive Honeypots using Reinforcement Learning Algorithms DQN and DDQN in Ensemble Framework: A Systematic Literature Review	1102
<i>Sohrab Farooq, Sadaf Hina, Sadaqat Rehman</i>	
Conditional Password Generation Using a FiLM-Enhanced WGAN: A Controlled Comparison Against Standard GAN Baselines.....	1109
<i>Pranav S Shetty, Pavan P, Srinivas P. M, Pruthvi C V, Vishal K Pujar</i>	
Interpretable Advanced Machine Learning Models for Early Identification of Health Insurance Claim Fraud Detection	1115
<i>Bhulakshmi Makkena</i>	
KyVul, an LLM Created C/C++ Vulnerability Dataset	1121
<i>Bryson Brown, Martin Carlisle</i>	
Poster: Automated SIEM Detection Rule Translation System	1129
<i>Adelia Ibragimova, Valentin Chichurov, Aleksandr Chikovani, Anton Tararykov</i>	
Reliable Extraction of Cyber-Physical System Threat Knowledge with Multi-Run LLMs	1132
<i>Lara Habashy, Illia Poplawski, Francois Rheume</i>	
Future-Proofing Cloud Infrastructure: AI/ML-Driven Automation for Predictive Cloud Operations.....	1140
<i>Vishwa Lakshnakiya</i>	
A Time-Series and Machine Learning Framework for Forecasting GDP and Unemployment Using Global Economic Indicators (2020–2024).....	1144
<i>Vidya Rajasekaran, Rajesh Vayyala, Krithika Rajendran, Baby Munirathinam, N.Arul N. Arul, G.Safiya Begam</i>	

FraudGNN: Self-Supervised Graph Neural Anomaly Detection for Real-Time Financial Fraud with Adversarial Robustness and Explainable Reasoning.....	1149
<i>Srikumar Nayak</i>	
TabNet-IDS: A TabNet-Driven Tabular Deep Learning Framework for Intrusion Detection Systems.....	1156
<i>Md Habibur Rahman, Md Wahidur Rahman, Avdesh Mishra, Tarek Mahmud, Mais Nijim</i>	
Agentic Metadata Cataloging for Power BI via LLM Scanners.....	1162
<i>Mohith Reddy Patlolla</i>	
Observability in Large-Scale Multi-Agent Ecosystems: Coordination, Emergence, and Failure Modes.....	1169
<i>Kailash Thiagarajan, Chirag Agrawal, Udaya Veeramreddygari</i>	
AI-Assisted Zero Trust Architecture for Continuous Risk Assessment of Programmable Logic Controllers in Food Processing Infrastructure.....	1175
<i>Sakshyam Ghimire</i>	
Privacy-Preserving Federated Deep Learning for Nomophobia Risk Prediction From Smartphone Usage Logs.....	1180
<i>Md Wahidur Rahman, Mehdi Hasan, Mais Nijim, Muhammad Armughan Ul Haq, Fawaz Ali Mohammed</i>	
A Federated Learning Framework for the IoMT System to Promote the Personalised Detection of COPD in a Non-Clinical Environment – A Pilot Study.....	1186
<i>Ramsha Ali</i>	
dataRLsec: Safety, Security, and Reliability With Robust Offline Reinforcement Learning for DPAs.....	1193
<i>Shriram KS Pandian, Naresh Kshetri</i>	
Exploring the Capabilities of LLMs in Binary Decompilation and Deobfuscation.....	1198
<i>Logan Mebane, Ajay Kumara Makanahalli Annaiah</i>	
Architecting for Privacy and Performance: A Federated Learning Framework for On-Device Financial AI in Mobile Applications	1204
<i>Ranjith Kumar Vanaparthi</i>	
Adversarial Machine Learning in Cybersecurity: Attacks, Defenses, Robustness, and Explainability	1209
<i>Sashidhar Chinthala</i>	
LLM-Assisted Codebook Development for Cybersecurity Interviews with Enhanced Accuracy and Reduced Hallucination	1213
<i>Aisvarya Adeseye, Jouni Isoaho, Seppo Virtanen, Mohammad Tahir</i>	
Hierarchical Attention Distillation for Real-Time Cyber Threat Detection and Mitigation in Large-Scale Networks.....	1219
<i>Ramkinker Singh, Om Narayan, Praveen Baskar, Sabitha Muppuri</i>	
BRUJO: Baseline-calibrated Risk from Unified Joint Observations for MITRE ATT&CK-based Time Series Forecasting in Security Operations Centers.....	1226
<i>Leonardo Octavio Perez-De La Torre, Andrew Wilson, Marco Perez-Cisneros, Gabriel Sanchez-Perez, Aldo Hernandez-Suarez</i>	
Cybersecurity Architecture for Cloud Database Infrastructure- A Case Study of Oracle Autonomous Database on Microsoft Azure	1232
<i>Chaitanya Kulkarni, Chandrashekhar Medicherla, Bharadwaj Vulugundam, Rajesh Purushothaman, Isan Sahoo, Arun Kumar Elengovan</i>	

AI-Powered Economic Digest and A Composite Index for National Financial Well-being: An AI-Driven Approach to Quantifying United States Financial Health with the USFHI	1238
<i>Bireswar Banerjee, Rajib Maitra</i>	
Cybersecurity in Blockchain-based fintech platforms: Social Perceptions and Adoption Intention.....	1242
<i>Md Sharif Hassan, Nguyen Hong Mai, Md Maruf Hassan, Abubokor Hanip</i>	
Multi-Frequency Implementation and Timing Analysis of LAES on Spartan-7 and Kintex-7 FPGAs	1248
<i>Keshav Kumar, Bishwajeet Pandey, Chinnaiyan Ramasubramanian</i>	
MBIST++: An Adaptive March Algorithm Generator for Memory Test Coverage Enhancement in Post-Silicon Validation	1253
<i>Deepika Bhatia</i>	
The Adaptive AI SOC Agent – Moving Beyond Linear Playbooks with Cognitive Reasoning	1259
<i>Valentin Chichurov, Adelia Ibragimova, Anton Tararykov</i>	
Bridging the Gap Using GPT-4 to Summarize and Explain Static Analysis Warnings at Scale	1262
<i>Arbaz Surti</i>	
Enhancing Trust in AI: Addressing Vulnerabilities and Ensuring Privacy with ML Security Protocols Across the Lifecycle	1268
<i>Ramkinker Singh, Om Narayan, Praveen Baskar</i>	
Mid-Generation Jailbreaks in Open-Source LLMs Using a Pause-and-Edit Attack.....	1279
<i>Aman Singh, Komal Subhash More, Samyam Aryal, Edward French, Mark Spanier</i>	
A Lightweight Deep Learning Based Classification Models for Non-Human Identity Threat Detection	1284
<i>Shiva Kumara</i>	
Secure Execution of Post Inference Scripts in AI Driven Vector Search Pipelines	1290
<i>Khrystyna Terletska, Kateryna Babii</i>	
Evaluating Adversarial Resilience of Deep Reinforcement Learning Algorithms for Network Intrusion Detection	1295
<i>Curtis Rookard</i>	
Prompting for LLM Security and RAG: A Survey from Zero-Shot to Automatic Prompt Optimization (APO) and Prompt-Injection Defenses	1301
<i>Ritesh Ruparel, Aravinda Jatavallabha, Srinivasa Maringanti</i>	

Author Index