

2025 IEEE 4th International Conference on AI in Cybersecurity (ICAIC 2025)

**Houston, Texas, USA
5-7 February 2025**



**IEEE Catalog Number: CFP25BD1-POD
ISBN: 979-8-3315-1889-9**

**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:	CFP25BD1-POD
ISBN (Print-On-Demand):	979-8-3315-1889-9
ISBN (Online):	979-8-3315-1888-2

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

A Novel Federated Learning Framework for Healthcare Applications using Wearable Devices	1
<i>Rajesh Natarajan, Sujatha Krishna, Christodoss P. Ranjith</i>	
Secure and Efficient Fraud Detection using Federated Learning and Distributed Search Databases.....	7
<i>Milavkumar Shah, Parth Shah, Swapnil Patil</i>	
Homomorphic Encryption in Federated Medical Image Classification.....	13
<i>Manuel Lengl, Simon Schumann, Stefan Röhl, Oliver Hayden, Klaus Diepold</i>	
Low Area Design and Implementation of Lightweight Encryption Algorithm on FPGA for IoT Devices	19
<i>Keshav Kumar, Chinnaiyan Ramasubramanian, Bishwajeet Pandey</i>	
Artificial Intelligence for Cybersecurity: A State of the Art	23
<i>Abdullah Al Siam, M. Maruf Hassan, Touhid Bhuiyan</i>	
SecureMedZK - A Blockchain-Based Approach with Zero-Knowledge Rollups for Secure EHR	30
<i>Darshika R. Pongallu, Shreyas S. Arun, Rohit Verma</i>	
Optimizing Intrusion Detection with Hybrid Deep Learning Models and Data Balancing Techniques.....	39
<i>M. Nasif Sarwar, M. Shohel Arman, Touhid Bhuiyan, Fatama B. Rafiq</i>	
Quantum Long Sort-Term Memory-Based Identification of Distributed Denial of Service Attacks.....	45
<i>Sarvapriya Tripathi, Himanshu Upadhyay, Jayesh Soni</i>	
Credit Card Fraud Detection using KNC, SVC, and Decision Tree Machine Learning Algorithms.....	53
<i>Pushpanjali Pandey, K. K. Garg</i>	
Cyber Attack Prediction on IoT and IIOT Devices using Ensemble Based Predictive Analytic Model	56
<i>Priyan M. Kumar, Tayyaba Shahwar, C. Gokulnath, Jeeva Selvaraj</i>	
Enhancing Trust Factor Identification in E-Commerce: The Role of Text Segmentation and Factor Extraction with Transformer Models.....	63
<i>Bandar F. Alkhalil, Yu Zhuang, Khalid T. Mursi, Ahmad O. Aseeri</i>	
Optimizing Route Efficiency in Formula One (F1) Vehicles using Reinforcement Learning Algorithms.....	71
<i>Sanam Narejo, Muhammad T. Khan, Muhammad Z. Shaikh, Lubna L. Dhirani, Bhawani S. Chowdhery</i>	
Time-Varying In-Hospital Mortality Prediction with Apache Spark	79
<i>Rohit S. Raja</i>	
Prediction of False Data Injection Attacks in Smart Grid using AdaBoost, Deep Learning, and KNN	85
<i>Bishwajeet Pandey, Nurkhat Zhakiyev, Madhu S. Gaur, Fariza Tumenbayeva, Sanjeev Kumar, Pushpanjali Pandey</i>	
Quantifying the Risk of Out-of-Gas Conditions in Ethereum Smart Contracts.....	89
<i>Maryam M. Ahmed, Michael Lim, Xiaorui Liu, Shen-Shyang Ho, Nikolay Ivanov</i>	

Promoting Health Through Transformative Innovation Policies and Emerging Technologies.....	97
<i>Rohit S. Raja</i>	
Quantifying Classification Metrics in Black Box Membership Inference Attacks	113
<i>Neil Dixit</i>	
Electronic Vehicle Charging and the Security Challenges of Renewable Energy Integration: An Optimization Framework.....	119
<i>Bryan Anderson, Gahangir Hossain</i>	
Rethinking the Place of African Kitchen Hut as a Hub for Business Management, Marketing, Education, Health and Strategies in the Age of Artificial Intelligence	125
<i>Chipo Mutongi, Billy Rigava, Tinashe Muchuri, Mufaro R. Chiwanza</i>	
Proactive AI-Driven Cybersecurity for Endangered Language Preservation: Safeguarding the Suba Linguistic Corpus	135
<i>Hesborn Ondiba</i>	
Future-Proofed Intrusion Detection for Internet of Things with Machine Learning	140
<i>Taiwo Adeyemi, Felix Ngobigha, Adnane Ez-Zizi</i>	
Explaining Cyber Risks in Transportaion 5.0: A Data Driven Approach	146
<i>Binod Tandan, Prashant Vajpayee, Gahangir Hossain</i>	
AdaPhish: AI-Powered Adaptive Defense and Education Resource Against Deceptive Emails	154
<i>Rei Meguro, Ng S. T. Chong</i>	
Mapping Cyber Threats in IoT-Driven MSPs: An Explainable Machine Learning Approach for Remote Work Security.....	161
<i>James Johnstone, Adewale Akinfaderin</i>	
A Metric for Measuring Distances Between Attack Trees in Cybersecurity	170
<i>Rohit S. Raja</i>	
Applying Communication Privacy Management Theory to Youth Privacy Management in AI Contexts.....	186
<i>Molly Campbell, Sandhya Joshi, Ankur Barthwal, Austin Shouli, Ajay K. Shrestha</i>	
Differential Privacy with DP-SGD and PATE for Intrusion Detection: A Comparative Study	196
<i>Daniel Machooka, Xiaohong Yuan, Kaushik Roy, Guenvere Chen</i>	
Using Large Language Models to Mitigate Human-Induced Bias in SMS Spam: An Empirical Approach	203
<i>Gerard S. Fuhnwi, Matthew Reville, Bradley Whitaker, Clemente Izurieta</i>	
Evaluating Text-Image Alignment using Gecko2K.....	210
<i>Aakarsh Etar, Jayesh Soni, Himanshu Upadhyay</i>	
Optimizing Cybersecurity Recruitment with Graph-Based Algorithms	216
<i>Jesudhas Yogarajah, Gahangir Hossain</i>	
AI2DS: Advanced Deep Autoencoder-Driven Method for Intelligent Network Intrusion Detection Systems.....	223
<i>M. Habibur Rahman, Leo Martinez, Avdesh Mishra, Mais Nijim, Ayush Goyal, David Hicks</i>	
AI-Driven Experiences: Exploring Consumer Purchase Intentions in a Social Context	229
<i>Shiu-Wan Hung, Jyun-Hao Jian, Che-Wei Chang, Jing-Ya Huang</i>	

Building Unique Interactive, Gamified Practical Exams for Cybersecurity Students	236
<i>Rashad Aliyev, Ziyafat Amirov, Alakbar Aliyev</i>	
Comparative Analysis of Federated Learning, Deep Learning, and Traditional Machine Learning Techniques for IoT Malware Detection	239
<i>Rami Darwish, Kaushik Roy</i>	
Generative AI for Automated Security Operations in Cloud Computing	249
<i>Advait Patel, Pravin Pandey, Hariharan Ragothaman, Ramasankar Molleti, Diwakar R. Peddinti</i>	
Securing Cloud AI Workloads: Protecting Generative AI Models from Adversarial Attacks	256
<i>Advait Patel, Pravin Pandey, Hariharan Ragothaman, Ramasankar Molleti, Ajay Tanikonda</i>	
Automated Detection of Malignant Lesions in the Ovary using Deep Learning Models and XAI	263
<i>M. H. S. Ifty, Nisharga Nirjan, Labib Islam, M. A. Diganta, Reeyad A. Ornate, Anika Tasnim, M. Saiful Islam</i>	
Transforming the Cybersecurity Space of Healthcare IoT Devices using Deep Learning	271
<i>Priyan M. Kumar, Balasubramanian P. Kavin, Abhignya Jagathpally, Tayyaba Shahwar</i>	
Out-of-Distribution Detection for Neurosymbolic Autonomous Cyber Agents	277
<i>Ankita Samaddar, Nicholas Potteiger, Xenofon Koutsoukos</i>	
Design and Analysis of Microstrip Patch Antenna using Metamaterial for Biomedical Applications	286
<i>Anshul Shrivastava, Rajesh Kumar, Kurmendra Singh</i>	
Lightweight Security Mechanism for IoT Applications using Substitution-Box.....	290
<i>Fozia Hanif, Rehan Shams, Urooj Waheed</i>	
Advanced Facial Emotion Classification with 135 Classes for Enhanced Cybersecurity Applications.....	296
<i>Gregory Powers, Aobo Jin, Abdul B. Tonmoy, Haowei Cao, Hardik Gohel, Qixin Deng</i>	
Air Pollutant (CO) Forecasting: A Hybrid Approach using Gooseneck Barnacle Optimization and Artificial Neural Networks	304
<i>Marzia Ahmed, Ahmad J. Mohamad, M. Maruf Hassan, Touhid Bhuiyan</i>	
Comparative Analysis of Password Alternatives for Enterprise Authentication: A Case Study	310
<i>Rahul Cherekar</i>	
Detection of Multiple Small Biased GPS Spoofing Attacks on Autonomous Vehicles	318
<i>Ahmad Mohammadi, Vahid Hemmati, Reza Ahmari, Frederick Owusu-Ambrose, Mahmoud N. Mahmoud, Abdollah Homaifar</i>	
A Framework of Dynamic Analysis of WannaCry	327
<i>Michael Cardoso, George Cardoso, Na Li</i>	
FocalCA: A Hybrid-Convolutional-Attention Encoder for Intrusion Detection on UNSW-NB15 Achieving High Accuracy Without Data Balancing	338
<i>Amin Amiri, Alireza Ghaffarnia, Shahnewaz K. Sakib, Dalei Wu, Yu Liang</i>	
A Comprehensive Security Orchestration, Automation, and Response System (SOAR) for Connected and Autonomous Vehicles (CAVs)	346
<i>Magani Niyomdi, Jared Oluoch</i>	

MAGICIAN: Malware Classification Approach Through Generation Image using a Conditional and wassersteIn Generative Adversarial Network Variants	360
<i>Stefano Galantucci, Andrea Iannacone, Giuseppe Pirlo, Lucia Sarcinella, Alessandro Stamerra</i>	
Addressing Vulnerabilities in AI-Image Detection: Challenges and Proposed Solutions.....	367
<i>Justin Jiang</i>	
Evaluation of Cybersecurity Awareness Level: A Case Study of Students of Sir Syed University of Engineering and Technology	376
<i>Fozia Hanif, Rehan Shams</i>	
Artificial Bee Colony Optimization Techniques’ Utilization for Intrusion Detection Systems’ Analysis	381
<i>Emre Tokgoz</i>	
Understanding the Threat of Political Deepfakes	397
<i>Kashifah Afroz, Swetha Chittam, Kaushik Roy</i>	
Secure Medical Imaging: A DICOM to JPEG 2000 Conversion Algorithm with Integrated Encryption	403
<i>Abdullah Al Siam, M. Maruf Hassan, Touhid Bhuiyan</i>	
A Multi-Level NLP Framework for Medical Concept Mapping in Healthcare AI Systems.....	409
<i>Rohit S. Raja</i>	
Machine Learning Techniques for Predicting the Increase in Municipal Solid Waste Generation in Lima, Perú	412
<i>Sandra-Evelia Garcia-Sandoval, Ciro R. Rodriguez</i>	
AI Agents for Cloud Reliability: Autonomous Threat Detection and Mitigation Aligned with Site Reliability Engineering Principles.....	421
<i>Mourya Chigurupati, Rajesh K. Malviya, Arvind R. Toorpu, Karanveer Anand</i>	
Silent Speech Interfaces: Non-Invasive Neuromuscular Signal Processing for Assistive Communication	425
<i>Sallar Khan, Khawaja U. Ali, Ali R. A. Qadri, Maisam Rizvi</i>	
C/C++ Vulnerability Data Set Generation Framework using a Parser and LLM	431
<i>Minh D. Nguyen, Martin Carlisle</i>	
Boosting Stock Predictions with Sentiment Analysis and Deep Learning Models.....	442
<i>Sarbanya R. Shakya, Edgar Ceh-Varela, Soneya Shakya, Caleb Parten, Zhaoxian Zhou</i>	
SQLSynthGen: Generating Synthetic Data for Healthcare Databases	448
<i>Rohit S. Raja</i>	
Low Field MRI Image Synthesis.....	459
<i>Kun Wang, Aobo Jin, Hongchun Guo, Yun Wan, Qixin Deng, Wenhui Chu, Maulin Raval, Hardik Gohel</i>	
Evaluating a Malware Benchmark Dataset using Neural Network Models and Shapley-Based Explainability	466
<i>Helen Qin, Shiyu Sun, Xiaohong Yuan</i>	

Model Inversion Attacks and Prevention Tactics using the HPCC Systems Platform.....	474
<i>Andrew B. A. Polisetty, Nandini S. Murthy, Yong Shi, Hugo Watanuki, Flavio Villanustre, Robert Foreman</i>	
Transforming Program Control Flow Data into Space-Filling Curves for Data Analysis	479
<i>Sebastian De La Cruz, Alexander Perez-Pons</i>	
Machine Learning Based Critical Velocity Predictions in Slurry Flows	488
<i>Ravi C. Mathi, Aparna Aravelli</i>	

Author Index