

# **2024 IEEE 3rd International Conference on AI in Cybersecurity (ICAIC 2024)**

**Houston, Texas, USA  
7 – 9 February 2024**



**IEEE Catalog Number: CFP24BD1-POD  
ISBN: 979-8-3503-8186-3**

**Copyright © 2024 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:	CFP24BD1-POD
ISBN (Print-On-Demand):	979-8-3503-8186-3
ISBN (Online):	979-8-3503-8185-6

**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](mailto:curran@proceedings.com)  
Web: [www.proceedings.com](http://www.proceedings.com)

CURRAN ASSOCIATES INC.  
**proceedings**  
.com

## TABLE OF CONTENTS

A Novel Deep Learning Method for Segmenting the Left Ventricle in Cardiac Cine MRI..... 1 <i>Wenhui Chu, Aobo Jin, Hardik A. Gohel</i>	1
Deep Reinforcement Learning-Based Malicious URL Detection with Feature Selection..... 10 <i>Antonio Maci, Nicola Tamma, Antonio Coscia</i>	10
AI-Based Cybersecurity Policies and Procedures ..... 17 <i>Shadi Jawhar, Jeremy Miller, Zeina Bitar</i>	17
AI-Driven Customized Cyber Security Training and Awareness ..... 22 <i>Shadi Jawhar, Jeremy Miller, Zeina Bitar</i>	22
A Secure Open-Source Intelligence Framework for Cyberbullying Investigation ..... 27 <i>Sylvia Worlali Azumah, Victor Adewopo, Zag Elsayed, Nelly Elsayed, Murat Ozer</i>	27
Improving Network Intrusion Detection Performance: An Empirical Evaluation using Extreme Gradient Boosting (XGBoost) with Recursive Feature Elimination ..... 35 <i>Gerard Shu Fuhnwi, Matthew Revelle, Clemente Izurieta</i>	35
YSAF: Yolo with Spatial Attention and FFT to Detect Face Spoofing Attacks..... 43 <i>Rathinaraja Jeyaraj, Barathi Subramanian, Karnam Yogesh, Aobo Jin, Hardik A. Gohel</i>	43
Leveraging Weak Supervision and BiGRU Neural Networks for Sentiment Analysis on Label-Free News Headlines..... 49 <i>Ahamadali Jamali, Shahin Alipour, Audrey Rah</i>	49
Identifying Race and Gender Bias in Stable Diffusion AI Image Generation ..... 54 <i>Aadi Chauhan, Taran Anand, Tanisha Jauhari, Arjav Shah, Rudransh Singh, Arjun Rajaram, Rithvik Vanga</i>	54
Toward Robust Systems Against Sensor-Based Adversarial Examples Based on the Criticalities of Sensors. .... 60 <i>Ade Kurniawan, Yuichi Ohsita, Masayuki Murata</i>	60
Secure Federated Learning Applied to Medical Imaging with Fully Homomorphic Encryption ..... 65 <i>Xavier Lessage, Leandro Collier, Charles-Henry Bertrand Van Ouytsel, Axel Legay, Saïd Mahmoudi, Philippe Massonet</i>	65
Federated Learning Based Smart Horticulture and Smart Storage of Fruits using E-Nose, and Blockchain: A Proposed Model ..... 77 <i>Shakhmaran Seilov, Bishwajeet Pandey, Akniyet Nurzhaubayev, Dias Abildinov, Assem Konyrkhanova, Bibinur Zhursinbek</i>	77
Video Key Concept Extraction using Convolution Neural Network..... 82 <i>Tanvir H Sardar, Ruhul Amin Hazarika, Bishwajeet Pandey, Guru Prasad M S, Sk Mahmudul Hassan, Radhakrishna Dodmane, Hardik Gohel</i>	82
CANAL - Cyber Activity News Alerting Language Model: Empirical Approach Vs. Expensive LLMs..... 88 <i>Urjithkumar Patel, Fang-Chun Yeh, Chinmay Gondhalekar</i>	88
Sentiment Analysis of Financial News Data using TF-IDF and Machine Learning Algorithms..... 100 <i>Gideon Popoola, Khadijat-Kuburat Abdullah, Gerard Shu Fuhnwi, Janet Agbaje</i>	100

Leveraging Advanced Visual Recognition Classifier for Pneumonia Prediction .....	106
<i>Maulin Raval, Jin Aobo, Yun Wan, Hardik Gohel</i>	
Simulations and Advancements in MRI-Guided Power-Driven Ferric Tools for Wireless Therapeutic Interventions .....	114
<i>Wenhui Chu, Aobo Jin, Hardik A. Gohel</i>	
DataAgent: Evaluating Large Language Models' Ability to Answer Zero-Shot, Natural Language Queries .....	124
<i>Manit Mishra, Abderrahman Braham, Charles Marsom, Bryan Chung, Gavin Griffin, Dakshesh Sidnerlikar, Chatanya Sarin, Arjun Rajaram</i>	
Prescriptive Analytics-Based Robust Decision-Making Model for Cyber Disaster Risk Reduction.....	129
<i>Joseph Ponnoly, John Puthenveetil, Patricia D'Urso</i>	
A Holistic Review on Detection of Malicious Browser Extensions and Links using Deep Learning .....	134
<i>Rama Abirami K, Tiago Zonta, Mithileysh Sathiyarayanan</i>	
zkFDL: An Efficient and Privacy-Preserving Decentralized Federated Learning with Zero Knowledge Proof.....	140
<i>Mojtaba Ahmadi, Reza Nourmohammadi</i>	
Navigating Data Privacy and Analytics: The Role of Large Language Models in Masking Conversational Data in Data Platforms .....	150
<i>Mandar Khoje</i>	
Mobile Application Security Risk Score: A Sensitive User Input-Based Approach.....	155
<i>Trishla Shah, Raghav Sampangi, Angela Siegel</i>	
Risk-Aware Mobile App Security Testing: Safeguarding Sensitive User Inputs .....	165
<i>Trishla Shah, Raghav Sampangi, Angela Siegel</i>	
Link-Based Anomaly Detection with Sysmon and Graph Neural Networks.....	173
<i>Charlie Grimshaw, Brian Lachine, Taylor Perkins, Emilie Coote</i>	
Addressing Data Imbalance in Plant Disease Recognition Through Contrastive Learning.....	179
<i>Bryan Chung</i>	
The Application of the Fifth Discipline Strategies in the Learning City Concept.....	185
<i>Chipo Mutongi, Billy Rigava</i>	
Robotics in Healthcare: The African Perspective .....	192
<i>Chipo Mutongi, Billy Rigava</i>	
Enhanced Network Intrusion Detection System using PCGSO-Optimized BI-GRU Model in AI- Driven Cybersecurity.....	202
<i>Priyan Malarvizhi Kumar, Kavya Vedantham, Jeeva Selvaraj, Balasubramanian Prabhu Kavin</i>	

## **Author Index**