

2025 International Conference on Artificial Intelligence Security and Governance (ICAISG 2025)

Hangzhou, China

12-14 December 2025

IEEE Catalog Number:
ISBN:

CFP257AX-POD
979-8-3315-5886-4



Copyright © 2025, 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:	CFP257AX-POD
ISBN (Print-On-Demand):	979-8-3315-5886-4
ISBN (Online):	979-8-3315-5885-7

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

Public Acceptance of Artificial Intelligence in China: Evidence From a National Survey*	1
<i>Delong Tang, Junping Hu, Yuele Huang, Lei Ren</i>	
ExpVLA: Enhancing the Generality of VLA Model via Explainable CoT Reasoning	5
<i>Ziyang Wang, Shengyang Wang</i>	
Q-Learning-Based Load Balancing for JSON-RPC Requests in Blockchain Networks	10
<i>Ba Ngoc Nguyen, Tuan-Dat Trinh</i>	
A Spatio-Temporal Gated Graph Attention Network with Structural Constraints	15
<i>Ze Zhao, Mingyan Jiang, Feng Wang</i>	
Advances on Memristor-Based Synaptic Component for Artificial Neural Network	20
<i>Lin Hua, Bangzhe Zhang, Xuefeng Ouyang, Zhongwei Wang, Yuanze Lyu</i>	
Self-Adaptive Thresholding for Semi-Supervised Multi-Modal Entity Alignment	30
<i>Jun Li, Lingxuan Zhu, Sunjie Huang</i>	
Agentic AI in DevOps: Boosting Software Automation and Collaboration	35
<i>Mohammed Akour, Mamdouh Alenezi</i>	
ML-Driven Unsupervised Software Malfunction Detection Using an Autoencoder	41
<i>Fedor Krasilnikov, Pavel Roganin, Zamira Kholmatova</i>	
Human-Centered Explainability in AI-Enhanced UI Security Interfaces: Designing Trustworthy Copilots for Cybersecurity Analysts	46
<i>Mona Rajhans</i>	
SAM: A Lightweight Static Attention Module for Kidney Stone Detection in CT Images	51
<i>Shukai Ding, Nirattaya Khamsemanan, Cholwich Nattee</i>	
ACA-Net: A Modified YOLOv11 Network for Accurate Wildlife Detection	56
<i>Shaode Yu, Xuemin Ren, Qiurui Sun</i>	
Smart Surveillance of Illegal Parking and Littering Detection Using Yolo-Based Machine Learning Algorithms in the Municipality of Los Baños	61
<i>Miguel Paulo C. Abella, Gene Marck B. Catedrilla</i>	
Privacy-Preserving and Efficient Aggregation for Federated Large Language Models	65
<i>Jing-Jing Li, Mingyang Fu, Xuanxuan Zhang, Jing Li, Jiliang Li</i>	
A CNN-RNN System for Real Time Credit Card Fraud Detection Using Three-Way Classification to Reduce False Positives /Negatives and Detect Fraud Across All Transaction Values	70
<i>David Maina, Merlin Kasirajan, Victor Obarafor</i>	
BAG-HRF: A Bayesian Attack Graph-Based Honeypoint Recommendation Framework	75
<i>Chenguang Wang, Rui Wang, Xin Deng, Xiang Yu, Mohan Li</i>	
AI-Driven Cybersecurity Threat Detection: A Hybrid CNN-LSTM Deep Learning Approach	80
<i>Haijia Zhong, Fucai Xie, Lanke Yu, Xianpeng Wang, Qi Xie, Mey Sok</i>	

Blockchain-Based Secure and Truthful Entity Participation Scheme in Heterogeneous Federated Learning	86
<i>Rui Wang, Xin Liu, Haojia Yang, Donglan Liu, Hao Zhang, Yiliang Liu, Zhou Su</i>	
Dark Web—Driven Threat Intelligence and Machine Learning—Powered Network Anomaly Detection for Automated Firewall Rule Management	91
<i>Yasin Çarkçi, Alperen Sayar, Seyit Ertuğrul, Gökem Demircan, Aslı Karabulut, Boran Ertuğrul</i>	
Backdoor Defense via Adversarial Resilience	97
<i>Xiaoxiao Chen, Yunlong Hu</i>	
Transferable Ensemble Black-Box Jailbreak Attacks on Large Language Models	102
<i>Xiaoxiao Chen, Jingwei Qian, Haitao Wang</i>	
Mitigating Backdoor Attacks via Attention Head Pruning	107
<i>Zhihong Liang, Kaitian Huang, Yuan Pan, Liang Xuan, Ximing Zhang, Wenqian Xu, Yiwei Yang</i>	
<i>Yixin Jiang, Peiming Xu, Leyu Bi</i>	
The Dual Role of Artificial Intelligence and LLM in Cybersecurity	113
<i>Leandros Maglaras, Vassilis C. Geroiannis, Mohamed Amine Ferrag, Alexios Lekidis</i>	
<i>Abderrahmane Lakas, Naghmeh Moradpoor</i>	