

2025 IEEE 12th International Conference on Cyber Security and Cloud Computing (CSCloud 2025)

**New York City, New York, USA
7-9 November 2025**



**IEEE Catalog Number: CFP25C21-POD
ISBN: 979-8-3315-8782-6**

**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:	CFP25C21-POD
ISBN (Print-On-Demand):	979-8-3315-8782-6
ISBN (Online):	979-8-3315-8781-9
ISSN:	2693-8952

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

2025 IEEE 12th International Conference on Cyber Security and Cloud Computing (CSCloud) **CSCloud 2025**

Table of Contents

Message from the General Chairs	xiv
Message from the Program Chairs	xv
Committee Members	xvi

CSCloud 1

Provenance-Based CTI Analysis with Knowledge Graph and RAG (KGRAG)	1
<i>Izuru Aki (Toyo University, Japan), Koki Watarai (Toyo University, Japan), Satoshi Okada (Toyo University, Japan), and Takuho Mitsunaga (Toyo University, Japan)</i>	
Hybrid Framework for Securing Machine to Machine Devices in Internet of Things (IOT)	7
<i>James Nyanumba Kimwomi (JKUAT, Kenya), Michael W. Kimwele (JKUAT, Kenya), and Felix Musau (JKUAT, Kenya)</i>	
Dynamic Feature Clustering for Anomaly Detection in Streaming Cybersecurity Data	13
<i>Christopher Hainzl (Ramapo College of New Jersey, USA), Sourav Dutta (Ramapo College of New Jersey, USA), Sheheeda Manakkadu (Gannon University, USA), and Ronny Bazan Antequera (Gannon University, USA)</i>	
A Longitudinal Security Analysis of Cloud Control Interfaces	19
<i>Victor Julio (Johns Hopkins University, USA), Ben Huang (Johns Hopkins University, USA), and Joel Coffman (Johns Hopkins University, USA)</i>	

CSCloud 2

Leveraging AVX Registers for Enhanced Encryption Security: The SecureKey Approach	25
<i>Jason Thomas (JET Technology Labs Inc, USA) and Ben Frehner (JET Technology Labs Inc., USA)</i>	
Intelligent Obstacle Resilience in Autonomous Vehicles Under Security Threats	34
<i>Chieh Tsai (University of Arizona, USA) and Hariri Salim (University of Arizona, USA)</i>	
ML-Aided Autonomous Cloud Platform Service Management Framework	42
<i>Manas Satish Singh (Stevens Institute of technology, USA), Noor Ahmed (Stevens Institute of Technology, USA), and Koushik Periyapatna Ravikumar (Stevens Institute of Technology, USA)</i>	

Explainable Multi-Modal Hybrid Framework for Cross-Domain Cyber-Physical Systems Security ...	48
<i>Srikanta Datta Tunkur (Indian Institute of Technology, Kanpur, USA), Jay Iyer (Coupang Global LLC, USA), and Sanjay Babu Kurra (Coupang Global LLC, USA)</i>	

CSCloud 3

KubeTrust: A Model for Automated Certificate Trust Management in Kubernetes	56
<i>Murat Kubilay (Deutsche Bank AG, Germany) and Sergey Shcherbakov (Google Germany GmbH, Germany)</i>	
Adaptive Hybrid GA-TS: Multi-Objective Task Scheduling for Enhanced Edge-Cloud Efficiency	62
<i>Joseph Reschelle Imbien (Oslo Metropolitan University (OsloMet), Norway) and Raju Shrestha (Oslo Metropolitan University (OsloMet), Norway)</i>	
Towards a Serverless Intelligent Firewall: AI-Driven Security, and Zero-Trust Architectures	68
<i>Md Anisur Rahman Chowdhury (Gannon University, USA), Hoang Nam Dang (Gannon University, USA), Ronny Bazan-Antequera (Gannon University, USA), Md. Sayham Khan (University of the Potomac, USA), Md Razaul Karim (University of the Potomac, USA), and Sheheeda Manakkadu (Gannon University, USA)</i>	
Class-Granular Attacks and Robust Defense in Federated Learning	74
<i>Md Faisal Ahmed (George Mason University), Zhuangdi Zhu (George Mason University), and Zhengdao Wang (George Mason University)</i>	

CSCloud 4

Probably Correct: Rethinking Formal Verification for LLM-Driven Systems	82
<i>Ayush Bhardwaj (Independent Researcher) and Sasha Fomina (Independent Researcher)</i>	
Privacy Through the Looking Glass: Diminished Reality to Enhance Privacy Beyond Reflective Leaks	87
<i>Salam Tabet (American University of Beirut, Lebanon), Kareem Bouakl (American University of Beirut, Lebanon), Zaynab Al Haj (American University of Beirut, Lebanon), Ayman Kayssi (American University of Beirut, Lebanon), Tim Allsopp (Telus Communications Inc., Canada), and Imad H. Elhajj (American University of Beirut, Lebanon)</i>	
Secure and Scalable AI Pipelines for Network Automation in Highly Regulated SaaS Environments	96
<i>Harika Rama Tulasi Karatapu (San Jose State University) and Vishal Gudhka (George Washington University)</i>	
A Dual-Branch CNN for Robust Detection of AI-Generated Facial Forgeries	100
<i>Xin Zhang (University of Southern Maine, USA), Yuqi Song (University of Southern Maine, USA), and Fei Zuo (University of Central Oklahoma, USA)</i>	

Self-Healing Application Architecture for Cloud-Based Environments	106
<i>Sri Tejaswi Gattupalli (Independent Researcher, USA), Rakshitha Mahesh Kumar (Independent Researcher, USA), and Bhavya Paliwal (Independent Researcher, USA)</i>	

CSCloud 5

ML-DaaS: An Integrated ML Training and Deployment Framework for Hybrid Cloud	110
<i>Koushik Periyapatna Ravikumar (Stevens Institute of Technology, USA), Noor Ahmed (Stevens Institute of Technology, USA), and Manas Satish Singh (Stevens Institute of Technology, USA)</i>	
Edge-Cloud Collaborative Privacy-Preserving Motion-Based Authentication for XR Systems	116
<i>Mingrui Yin (New Jersey Institute of Technology, USA), Sohom Sen (New Jersey Institute of Technology, USA), Yongjie Guan (University of Maine, USA), Xueyu Hou (University of Maine, China), Tao Han (New Jersey Institution of Technology), and Nirwan Ansari (New Jersey Institute of Technology, USA)</i>	
Casper: Prompt Sanitization for Protecting User Privacy in Web-Based Large Language Models.....	122
<i>Chun Jie Chong (New Jersey Institute of Technology, USA), Chenxi Hou (New Jersey Institute of Technology, USA), Zhihao Yao (New Jersey Institute of Technology, USA), and Seyed Mohammadjavad Seyed Talebi (Independent Researcher, USA)</i>	
Graph-Structured Learning for Cyber Intrusion Detection in Electric Vehicle Charging Systems	134
<i>Yujung Hwang (University at Albany, SUNY), Furkan Kurt (University at Albany, SUNY), and Abdulhamit Subasi (University at Albany, SUNY)</i>	
HEAPE: A Novel Hybrid Adaptive Embedding Engine Architecture for Cybersecurity and Anomaly Detection in Cloud Logs using Java and LangChain4J	140
<i>Alok Tibrewala (The George Washington University, USA,)</i>	

CSCloud 6

Ensuring Fair Credit Access with Algorithmic Transparency	149
<i>Leela Krishna Yenigalla (Independent Researcher, USA)</i>	
Leveraging LLMs for Detecting Security Threats in Virtual Network Functions	154
<i>Ibrahim Khalil Mejri (University of Trento, Italy) and Sara Sutton (Grand Valley State University, USA)</i>	
Scheduling and Transaction Management of Control Commands for Logical Actuators on Logical IoT Cloud	160
<i>Takayuki Kushida (Tokyo University of Technology, Japan) and Yuka Kato (Tokyo Woman's Christian University, Japan)</i>	
Evaluating Functional Package Management and Containerization for Scalable Software Development and Deployment: A Comparative Study	166
<i>Praveen Kumar Sayani (Independent Researcher)</i>	

Threat Modeling and LLM-Based Anomaly Detection for Fog Computing Service Function Chains	173
---	-----

Sara Sutton (Grand Valley State University, USA), Fahim Morshed (Grand Valley State University, USA), and Trevor Ouma (Grand Valley State University, USA)

Generating Context-Aware Cyberbullying Dialogues: A Structured LLM-Based Dataset	179
--	-----

Mohammad Shafiqul Islam (Grand Valley State University, USA), Sara Sutton (Grand Valley State University, USA), and Rahat Ibn Rafiq (Grand Valley State University, USA)

CSCloud 7

An Empirical Study of Google's Advertising Ecosystem: From User Profiling to Ad Targeting	185
---	-----

Tianming Zheng (Academy of Cyber, China), Hua Li (Beijing Shuimu Wangjing Technology, China), Shu Meng (Zhejiang University, China), Haitao Xu (Zhejiang University, China), Zhao Li (Hangzhou Yugu Technology, China), and Shichang Hu (Hangzhou Yugu Technology, China)

Scalable Cloud Architecture for Computational Microscopy: A Microservices Approach with Dynamic Resource Management	191
---	-----

Moran Xu (Carl Zeiss X-ray Microscopy, Inc., USA), Aman Garg (Georgia Institute of Technology, USA), Felix Scheffler (Carl Zeiss Microscopy GmbH), Shiqi Xu (Carl Zeiss X-ray Microscopy, Inc., USA), Faguo Yang (Carl Zeiss X-ray Microscopy, Inc., USA), Matthew Andrew (Carl Zeiss X-ray Microscopy, Inc., USA), and Andriy Andreyev (Carl Zeiss X-ray Microscopy, Inc., USA)

Latency-Aware Mechanism for Deep Learning-Based Network Intrusion Detection	196
---	-----

Colum Chen (City of London Freeman's School, United Kingdom) and Michael Huang (Harrow International School Shenzhen, China)

Deep Learning for Face Deblurring: A Survey	202
---	-----

Heye Wu (Minzu University of China, China), Jing Yu (Minzu University of China, China), Kexin Wang (Minzu University of China, China), Yihang Wei (Beijing Institute of Technology, China), Qianhang Niu (Minzu University of China, China), Yijun Cong (Minzu University of China, China), and Keke Gai (Beijing Institute of Technology, China)

CSCloud 8

Real-Time Traffic Detection for Lightweight Blockchain	208
--	-----

Shaolong Tang (Beijing Institute of Technology, China), Peng Jiang (Beijing Institute of Technology, China), and Liehuang Zhu (Beijing Institute of Technology, China)

MGA-KGF: A Multi-Granularity Adaptive Knowledge Graph Fusion Framework for Heterogeneous Multi-Source Smart Grid Data	214
<i>Zhongyan Chai (Peking University, China), Zhongjun Wang (Southern Power Grid Digital Platform Technology Company Limited, China), Weiwei Li (China Southern Power Grid Company Limited, China), Yang Yang (Southern Power Grid Digital Platform Technology Company Limited, China), Dazhong Wu (Southern Power Grid Digital Platform Technology Company Limited, China), and Fengbo Wu (Southern Power Grid Digital Platform Technology Company Limited, China)</i>	
A Survey on Image Immunization Techniques	221
<i>Hanqing Zhang (Minzu University of China, China), Jing Yu (Minzu University of China, China), Zhipeng Ru (Minzu University of China, China), Yihang Wei (Beijing Institute of Technology, China), Jiaoyang Su (Minzu University of China, China), Lizhi Zhao (Minzu University of China, China), and Keke Gai (Beijing Institute of Technology, China)</i>	
Rowing in Sync: A Data-Driven Model to Uncover Synchronization Gaps in Team Performance	227
<i>Hanhua Hu (Ridley College) and Sherrie Buchner (Ridley College)</i>	

CSCloud 9

Application Research and Trend Analysis of the Industrial Internet Identification and Resolution System	232
<i>Chuangchuang Dai (China Academy of Safety Science and Technology, China), Guangkuo Cao (China Academy of Safety Science and Technology, China), Yucheng Li (China Academy of Safety Science and Technology, China), Qiang Zhao (China Academy of Safety Science and Technology, China), Dong Xu (China Academy of Safety Science and Technology, China), Baoqing Wang (China Academy of Safety Science and Technology, China), and Lei Guan (China Academy of Safety Science and Technology, China)</i>	
Multi-Modal Image Fusion with State Space Mamba Networks	238
<i>Yulin Gu (Digital Platform Technology Co., Ltd., China), Shijie Li (China Southern Power Grid Co., Ltd., China), Fengbo Wu (Digital Platform Technology Co., Ltd., China), Dazhong Wu (Digital Platform Technology Co., Ltd., CSG, Shenzhen, China), Qing Cao (Digital Platform Technology Co., Ltd., China), Xin Chen (Digital Platform Technology Co., Ltd., China), Jiazhong Zhang (Digital Platform Technology Co., Ltd., China), and Yiwei Lou (Peking University, China)</i>	
Time Series Anomaly Detection: A Hybrid Deep Learning Framework with Adaptive Thresholding for Electricity Industry Data	244
<i>Yifan Xiao (Peking University, China), Zhongjun Wang (China Southern Power Grid Digital Platform Technology Company, China), Tiantian Yan (China Southern Power Grid Company Limited, China), Weiwei Li (China Southern Power Grid Digital Platform Technology Company, China), Dazhong Wu (China Southern Power Grid Digital Platform Technology Company, China), and Jie Ma (China Southern Power Grid Digital Platform Technology Company, China)</i>	

AstraMPC: Asynchronous Data-Driven Framework for Multi-Party Secure Computation	250
<i>Shuning Sun (University of Chinese Academy, China), Xiaojie Xu (Hangzhou Qulian Technology Co., Ltd., China), Jianghao Chen (University of Chinese Academy of Sciences, China), Mengyao Zhao (University of Chinese Academy of Sciences, China), Huijun Zhang (Digital Silk Road Xinjiang Industry Investment Group Company, China), and Xiaofeng Chen (State Key Laboratory of Blockchain and Data Security (Zhejiang University); Chongqing Qulian Digital Technology Co., Ltd; Hangzhou Qulian Technology Co., Ltd., China)</i>	

CSCloud 10

EG-DAG: Efficient Federated Learning Framework Based on Guided Directed Acyclic Graph	258
<i>Xiangfei Lou (Hangzhou Qulian Technology Co., Ltd, China), Xiaofeng Chen (Zhejiang University; Hangzhou Qulian Technology Co., Ltd.; Chongqing Qulian Digital Technology Co., Ltd., China), Yijian Zhang (Hangzhou Julian Technology Co., Ltd, China), Xiaojie Xu (Hangzhou Qulian Technology Co., Ltd, China), Wenfei Ge (Hangzhou Qulian Technology Co., Ltd., China), and Huijun Zhang (Digital Silk Road Xinjiang Industry Investment Group Company, China)</i>	

Real-Time Self-Adaptive SMPC for Non-IID Vehicular Data in Intelligent Transportation Systems	266
---	-----

Xiaojie Xu (Hangzhou Qulian Technology Co., Ltd., China), Xiaofeng Chen (State Key Laboratory of Blockchain and Data Security (Zhejiang University); Chongqing Qulian Digital Technology Co., Ltd; Hangzhou Qulian Technology Co., Ltd., China), Xiangfei Lou (Hangzhou Qulian Technology Co., Ltd., China), Ziling Liu (Hangzhou Qulian Technology Co., Ltd., China), Yijian Zhang (Zhejiang University, China), and Huijun Zhang (Digital Silk Road Xinjiang Industry Investment Group Company, China)

DEL: A Fine-Grained Power Consumption Estimation Model Integrating Deep & Cross Network with LSTM	274
---	-----

Zhu Chunqiang (State Grid Shaanxi Electric Power Co., Ltd.Training Center Digital Work Department, China), Wang Jing (State Grid Shaanxi Electric Power Co., Ltd.Training Center Digital Work Department, China), and Quan Wei (State Grid Shaanxi Electric Power Co., Ltd.Training Center Digital Work Department, China)

CSCloud 11

A Spatio-temporal Correlation Data Model for Improving Panoramic Monitoring Performance within Source-Grid-Load-Storage Systems	280
---	-----

Wang Jing (State Grid Shaanxi Electric Power Co., Ltd.Training Center Digital Work Department, China), Zhu Chunqiang (State Grid Shaanxi Electric Power Co., Ltd.Training Center Digital Work Department, China), Zhao Kaihang (State Grid Shaanxi Electric Power Co., Ltd.Training Center Digital Work Department, China), Quan Wei (State Grid Shaanxi Electric Power Co., Ltd.Training Center Digital Work Department, China), and Mou Xudong (Beihang University, China)

Cross-Modal Physiological Sound Recognition in Smart Healthcare Scenarios: Dataset Construction for Real-Time Monitoring and Deep Learning Classification Methods	286
<i>Xiaodong Zheng (Xiamen University of Technology, China), Jingyu Yan (VN Karazin Kharkiv National University, Ukraine), Wei Zhu (Xiamen University of Technology, China), and Chengye Li (Central South University, China)</i>	
Explainable AI-Enabled Intrusion Detection Systems for Computer Networks	292
<i>Dakshnamoorthy Manivannan (University of Kentucky, USA)</i>	
Data Deduplication Techniques: Advantages, Disadvantages, Open Issues, and Future Directions	298
<i>Dakshnamoorthy Manivannan (University of Kentucky, USA)</i>	

CSCloud 12

Advancing Network Security in 5G: Leveraging the 5G-NIDD Dataset for Intrusion Detection and Mitigation	304
<i>Sachin Singh (Independent Researcher)</i>	
NebulaX: Scalable Cross-Chain Interoperability via zk-SNARK Aggregation and Dynamic Incentives	310
<i>Wenfei Ge (Hangzhou Qulian Technology Co., Ltd., China), Xiaofeng Chen (State Key Laboratory of Blockchain and Data Security (Zhejiang University); Chongqing Qulian Digital Technology Co., Ltd; Hangzhou Qulian Technology Co., Ltd., China), Jianghao Chen (Hangzhou Qulian Technology Co., Ltd., China), Xiangfei Lou (Hangzhou Qulian Technology Co., Ltd., China), Xiaojie Xu (Hangzhou Qulian Technology Co., Ltd., China), and Huijun Zhang (Digital Silk Road Xinjiang Industry Investment Group Company, China)</i>	
Model-Free Zero Trust Defense Method Based on Recurrent Actor-Critic Framework	320
<i>Yusi Cheng (University of Science and Technology, China), Jie Sun (Zhongguancun laboratory, China), Bo Li (Beihang University, China), and Qihao Lu (Zhongguancun laboratory, China)</i>	

CSCloud Special Track 1

Hybrid DRL and Market Regime Identification for Optimal Uniswap V3 Liquidity Provision	326
<i>Cheng-Tai Huang (National Tsing Hua University, Taiwan), Wei-Ru Chen (Independent Researcher, Taiwan), and Shen-Ning Tung (National Tsing Hua University, Taiwan)</i>	
Policy Induction: Predicting Startup Success via Explainable, Memory-Augmented In-Context Learning	331
<i>Xianling Mu (University of Oxford, UK), Joe Ternasky (Vela Research, USA), Fuat Alican (Vela Research, USA), Rick Chen (University of Oxford, UK), and Yigit Ihlamur (Vela Research, USA)</i>	
Multi-Agent Deep Reinforcement Optimization for Crypto Trading	335
<i>Ch Hamza Akbar (Technische Universität Dresden, Germany)</i>	

FinVerse Agent: Resource-Efficient Financial LLMs with Modular LoRA Fine-Tuning and Task Routing	338
<i>Laiba Rana (National University of Sciences and Technology (NUST), Pakistan), Ahmed Amin (Zewail City University, Egypt), Huma Ameer (National University of Sciences and Technology (NUST), Pakistan), and Seemab Latif (National University of Sciences and Technology (NUST), Pakistan)</i>	
FinGPT: Agent for Real-World Financial Analytics: Cross-Domain Enhancement with FinLoRA	341
<i>Zifan Dong (Northwestern University, USA), Kaiyuan Yang (Northwestern University, USA), Bingye Liu (Northwestern University, USA), and Tong Su (Northwestern University, USA)</i>	

CSCloud Special Track 2

DeFi Liquidity Provisioning with Reinforcement Learning and Dynamic Feature Selection	344
<i>Benoît-Marie Robaglia (Independent Researcher, France)</i>	
FinRL-DT: Financial Reinforcement Learning Using Decision Transformers	347
<i>Bojun Liu (Columbia University, USA), Keyi Wang (Columbia University, USA), Anwar Walid (Columbia University, USA), and Xiao-Yang Liu Yanglet (SecureFinAI Lab, Columbia University)</i>	
Reasoned Rule Mining: Precision-Optimised Weighted LogProb Classification	351
<i>Jack Preuveneers (University of Oxford, Oxford) and Yigit Ihlamur (Vela Research, USA)</i>	
FinGPT Agents: Reinforcement-Fine-Tuned LLMs for Financial Analytics	355
<i>Satish Chandra (Anurag University, India) and G. Balakrishna (Anurag University, India)</i>	
FinAI-Trader: Sentiment-Enhanced Reinforcement Learning for Bitcoin Trading in the FinAI Contest 2025 Task 1	358
<i>Taimoor Ahmed (National University of Sciences and Technology (NUST), Pakistan), Nikhar Azhar (National University of Sciences and Technology (NUST), Pakistan), Sahar Arshad (National University of Sciences and Technology (NUST), Pakistan), and Mehwish Fatima (National University of Sciences and Technology (NUST), Pakistan)</i>	

CSCloud Special Track 3

Parallel Environments for Traveling Salesman Problems Using Reinforcement Learning	361
<i>Ming Zhu (University of Chinese Academy of Sciences, China) and Zhiqiang Pu (University of Chinese Academy of Sciences, China)</i>	
Parallel Environments for Graph Maxcut Using Reinforcement Learning	364
<i>Shaohua Hu (Beijing Jiaotong University, China), Ming Zhu (University of Chinese Academy of Sciences, China), and Zhiqiang Pu (University of Chinese Academy of Sciences, China)</i>	
Parallel Environments for Combinatorial Optimization Problems Using Reinforcement Learning...	367
<i>Ming Zhu (University of Chinese Academy of Sciences, China) and Zhiqiang Pu (University of Chinese Academy of Sciences, China)</i>	

Author Index 371