

# **2024 IEEE 23rd International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom 2024)**

**Sanya, China  
17-21 December 2024**

**Pages 1-682**



**IEEE Catalog Number: CFP24TRU-POD  
ISBN: 979-8-3315-0621-6**

**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:	CFP24TRU-POD
ISBN (Print-On-Demand):	979-8-3315-0621-6
ISBN (Online):	979-8-3315-0620-9
ISSN:	2324-898X

**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

# 2024 IEEE 23rd International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom) TrustCom/BigDataSE/CSE/ECU/iSCI 2024

## Table of Contents

Message from the TrustCom 2024 Steering Chairs .....	lviii
Message from the TrustCom 2024 General Chairs .....	lix
Message from the TrustCom 2024 Program Chairs .....	lx
Message from the BigDataSE 2024 Steering Chairs .....	lxi
Message from the BigDataSE 2024 General Chairs .....	lxii
Message from the BigDataSE 2024 Program Chairs .....	lxiii
Message from the CSE 2024 Steering Chairs .....	lxiv
Message from the CSE 2024 General Chairs .....	lxv
Message from the CSE 2024 Program Chairs .....	lxvi
Message from the EUC 2024 Steering Chairs .....	lxvii
Message from the EUC 2024 General Chairs .....	lxviii
Message from the EUC 2024 Program Chairs .....	lxix
Message from the iSCI 2024 Steering Chairs .....	lxx
Message from the iSCI 2024 General Chairs .....	lxxi
Message from the iSCI 2024 Program Chairs .....	lxxii
TrustCom 2024 Organizing Committee .....	lxxiii
TrustCom 2024 Program Committee .....	lxxiv
BigDataSE 2024 Organizing Committee .....	lxxxii
BigDataSE 2024 Program Committee .....	lxxxiii
CSE 2024 Organizing Committee .....	lxxxiv
CSE 2024 Program Committee .....	lxxxv
EUC 2024 Organizing Committee .....	lxxxvii
EUC 2024 Program Committee .....	lxxxviii
iSCI 2024 Organizing Committee .....	lxxxix
iSCI 2024 Program Committee .....	xc

## The 23rd IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom 2024)

### TrustCom-1: Trust (I)

MAXPoWR: Memory Attestation and Export in Process-Based Trusted Execution Environments .....	1
<i>Hendrik Meyer Zum Felde (Fraunhofer AISEC, Germany) and Andrei-Cosmin Aprodu (Fraunhofer AISEC, Germany)</i>	

Trusted Networking for Drones: Reputation-Based Security Mechanisms for Node Access and Information Synchronization .....	13
<i>Ruizhong Du (Hebei University, China), Jiajia Kang (Hebei University, China), and Jin Tian (Hebei University, China)</i>	
Enhancing Consistency in Container Migration via TEE: A Secure Architecture .....	21
<i>Qingyu Gao (National University of Defense Technology, China), Liantao Song (National University of Defense Technology, China), Yan Lei (Chongqing University, China), Feng Wang (Hunan University, China), Lei Wang (National Innovation Institution of Defense Technology, China), Shize Zong (National University of Defense Technology, China), and Yan Ding (National University of Defense Technology, China)</i>	
A Semi-Fragile Reversible Watermarking for 3D Models Based on IQIM with Dual-Strategy Partition Modulation .....	29
<i>Fei Peng (Guangzhou University, China), Yousheng Liang (Guangzhou University, China), and Min Long (Guangzhou University, China)</i>	
MSMP: A Centralized Shared-Memory Management for Building Efficient and Reliable File Systems on Microkernels .....	37
<i>Feng He (Institute of Information Engineering, Chinese Academy of Sciences; University of Chinese Academy of Sciences, China), Shijun Zhao (Institute of Information Engineering, Chinese Academy of Sciences, China), Dan Meng (Institute of Information Engineering, Chinese Academy of Sciences, China), and Rui Hou (Institute of Information Engineering, Chinese Academy of Sciences, China)</i>	
Blind Signature Based Anonymous Authentication on Trust for Decentralized Mobile Crowdsourcing .....	49
<i>Wei Feng (Xi'an Jiaotong University, China), Dongyuan Wei (Xi'an Jiaotong University, China), and Qianqian Wang (Xidian University, China)</i>	

## TrustCom-2: Security (I)

CTWF: Website Fingerprinting Attack Based on Compact Convolutional Transformer .....	57
<i>Guangfa Lyu (Shandong University, China), Jian Kong (Shandong University, China), Yinglong Chen (Shandong University, China), and Fengyu Wang (Shandong University, China; Quan Cheng Laboratory, China)</i>	
LSTM-Diff: A Data Generation Method for Imbalanced Insider Threat Detection .....	68
<i>Tian Tian (Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China), Yan Zhu (Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China), Ning An (Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China), Bo Jiang (Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China), Huamin Feng (Beijing Electronic Science and Technology Institute, China), and Zhigang Lu (Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China)</i>	

SeChannel: A Secure and Lightweight Channel Protection Approach for TEE Systems .....	77
<i>Nan Jiang (Chinese Academy of Sciences; University of Chinese Academy of Sciences, China), Yuanbo Zhao (Chinese Academy of Sciences; University of Chinese Academy of Sciences, China), Qihang Zhou (Chinese Academy of Sciences, China), Xiaoqi Jia (Chinese Academy of Sciences; University of Chinese Academy of Sciences, China), and Jing Tang (Chinese Academy of Sciences, China)</i>	
Hardware Assisted Security Gateway System: Combined with FPGA Shielding Protection .....	85
<i>Jihong Liu (Chinese Academy of Sciences, China; Key Laboratory of Cyberspace Security Defense, China; University of Chinese Academy of Sciences, China), Chenyang Tu (Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China), and Yifei Zhang (Chinese Academy of Sciences, China; Key Laboratory of Cyberspace Security Defense, China)</i>	
xIDS-EnsembleGuard: An Explainable Ensemble Learning-Based Intrusion Detection System .....	93
<i>Muhammad Adil (University at Buffalo, USA), Mian Ahmad Jan (University of Sharjah, UAE), Safayat Bin Hakim (University of Maryland, USA), Houbing Herbert Song (University of Maryland, USA), and Zhanpeng Jin (South China University of Technology Guangdong, China; University at Buffalo, USA)</i>	
DMA: A Persistent Threat to Embedded Systems Isolation .....	101
<i>Jean de Bonfils Lavernelle (University of Limoges, France; Thales DIS, France), Pierre-François Bonnefoi (University of Limoges, France), Benoît Gonzalvo (Thales DIS, France), and Damien Sauveron (University of Limoges, France)</i>	

## **TrustCom-3: Security (II)**

StegaFDS: Generative Steganography Based on First-Order DPM-Solver .....	109
<i>Chengyu Li (University of Science and Technology of China, China), Weihai Li (University of Science and Technology of China, China), Zikai Xu (University of Science and Technology of China, China), and Nenghai Yu (University of Science and Technology of China, China)</i>	
Red Team Redemption: A Structured Comparison of Open-Source Tools for Adversary Emulation .....	117
<i>Max Landauer (Austrian Institute of Technology, Austria), Klaus Mayer (Austrian Institute of Technology, Austria), Florian Skopik (Austrian Institute of Technology, Austria), Markus Wurzenberger (Austrian Institute of Technology, Austria), and Manuel Kern (Austrian Institute of Technology, Austria)</i>	
VisualAuth: Secure Transaction Authentication and Trusted UI on COTS Android Devices .....	129
<i>Mykolai Protsenko (Fraunhofer AISEC, Germany), Albert Stark (Fraunhofer AISEC, Germany), Andreas Papon (ETH Zurich, Switzerland), and Sandra Kostic (Fraunhofer AISEC, Germany)</i>	

From Data to Action: CTI Analysis and ATT&CK Technique Correlation .....	141
<i>Khanh-Duy Nguyen (National Central University, Taiwan), Hsi-Ching Chu (National Central University, Taiwan), Quoc-Viet Nguyen (National Central University, Taiwan), Min-Te Sun (National Central University, Taiwan), Kazuya Sakai (Tokyo Metropolitan University, Japan), and Wei-Shinn Ku (Auburn University, USA)</i>	
A Revocable Pairing-Free Certificateless Signature Scheme Based on RSA Accumulator .....	149
<i>Zhuowei Shen (Southeast University, China; Minster of Education, China), Xiao Kou (Southeast University, China), Taiyao Yang (Southeast University, China), Haoqin Xu (Southeast University, China), Dongbin Wang (Beijing University of Post and Telecommunications, China; Ministry of Education, China), and Shaobo Niu (Southeast University, China)</i>	
Face Anti-Spoofing Based on Multi-Modal Dual-Stream Anomaly Detection .....	157
<i>Jiuyao Jing (Xidian University, China), Yu Zheng (Xidian University, China), Qi He (Xidian University, China), and Chunlei Peng (Xidian University, China)</i>	

#### **TrustCom-4: Security (III)**

Behavior Speaks Louder: Rethinking Malware Analysis Beyond Family Classification .....	165
<i>Fei Zhang (Tianjin University, China), Xiaohong Li (Tianjin University, China), Sen Chen (Tianjin University, China), and Ruitao Feng (Southern Cross University, Australia)</i>	
Vulnerabilities are Collaborating to Compromise Your System: A Network Risk Assessment Method Based on Cooperative Game and Attack Graph .....	176
<i>Xin Deng (Beijing University of Posts and Telecommunications, China; Peng Cheng Laboratory, China), Rui Wang (Guangzhou University, China), Weihong Han (Peng Cheng Laboratory, China), and Zhihong Tian (Guangzhou University, China)</i>	
StegoFL: Using Steganography and Federated Learning to Transmit Malware .....	184
<i>Rong Wang (Sichuan Normal University, China; Hosei University, Japan), Junchuan Liang (Sichuan Normal University, China), Haiting Jiang (Sichuan Normal University, China), Chaosheng Feng (Sichuan Normal University, China), and Chin-Chen Chang (Feng Chia University, Taiwan)</i>	
Correcting the Bound Estimation of Mohawk .....	191
<i>Mingjie Yu (University of Science and Technology of China, China; Chinese Academy of Sciences, China; Key Laboratory of Cyberspace Security Defense, China), Wei Jin (China Academy of Information and Communications Technology, China), Fenghua Li (University of Science and Technology of China, China; Chinese Academy of Sciences, China; Key Laboratory of Cyberspace Security Defense, China; University of Chinese Academy of Sciences, China), Yunchuan Guo (Chinese Academy of Sciences, China; Key Laboratory of Cyberspace Security Defense, China; University of Chinese Academy of Sciences, China), Zheng Yan (Xidian University, China), Xiao Wang (Chinese Academy of Sciences, China; Key Laboratory of Cyberspace Security Defense, China; University of Chinese Academy of Sciences, China), and Nenghai Yu (University of Science and Technology of China, China)</i>	

OFLGI: An Optimization-Based Feature-Level Gradient Inversion Attack .....	197
<i>Yongwei Lu (Hebei University, China; Key Lab on High Trusted Information System of Hebei Province, China), Xiaoyan Liang (Hebei University, China; Key Lab on High Trusted Information System of Hebei Province, China), Ruizhong Du (Hebei University, China; Key Lab on High Trusted Information System of Hebei Province, China), and Junfeng Tian (Hebei University, China; Key Lab on High Trusted Information System of Hebei Province, China)</i>	

Front-Running Attacks in Hash-Based Transaction Sharding Blockchains .....	205
<i>Yusen Wang (Shanghai Jiao Tong University, China), Jiong Lou (Shanghai Jiao Tong University, China; Shanghai Jiao Tong University (Wuxi) Blockchain Advanced Research Center, China; Shanghai Key Laboratory of Trusted Data Circulation and Governance and Web3, China), Zihan Wang (Shanghai Jiao Tong University, China), and Jie Li (Shanghai Jiao Tong University, China; Shanghai Jiao Tong University (Wuxi) Blockchain Advanced Research Center, China; Shanghai Key Laboratory of Trusted Data Circulation and Governance and Web3, China)</i>	

## TrustCom-5: Security (IV)

Multi-Authority Ciphertext-Policy Attribute-Based Encryption with Hidden Policy for Securing Internet-of-Vehicles .....	213
<i>Jie Cui (Anhui University, China), Jing Zhang (Anhui University, China), Lu Wei (Anhui University, China), Minghui Zhu (Anhui University, China), Hong Zhong (Anhui University, China), and Geyong Min (University of Exeter, UK)</i>	

WASHADOW: Effectively Protecting WebAssembly Memory Through Virtual Machine-Aware Shadow Memory .....	222
<i>Zhuochen Jiang (University of Science and Technology of China, China) and Baojian Hua (University of Science and Technology of China, China)</i>	

Attacking High-Performance SBCs: A Generic Preprocessing Framework for EMA .....	234
<i>Debao Wang (Nanjing University of Science and Technology, China), Yiwen Gao (Nanjing University of Science and Technology, China), Jingdian Ming (Nanjing University of Science and Technology, China; Zhejiang University, China), Yongbin Zhou (Nanjing University of Science and Technology, China; Chinese Academy of Sciences, China), and Xian Huang (Open Security Research, China)</i>	

CPCED: A Container Escape Detection System Based on CNI Plugin .....	242
<i>Yu Hao (Beijing University of Posts and Telecommunications, China), Xu Zhang (Beijing University of Posts and Telecommunications, China), and Dongbin Wang (Beijing University of Posts and Telecommunications, China)</i>	

Path Generation Method of Anti-Tracking Network Based on Dynamic Asymmetric Hierarchical Architecture .....	254
<i>Zhefeng Nan (Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China), Qi Wang (National Computer Network Emergency Response Technical Team/Coordination Center, China), Changbo Tian (Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China), Yijing Wang (Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China), Tianning Zang (Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China), and Dongwei Zhu (Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China)</i>	
TOScorr: Transformer-Based Flow Correlation Attack on Tor Onion Service .....	262
<i>Yilin Zhu (Southeast University, China), Guang Cheng (Southeast University, China), Shunyu Zheng (Southeast University, China), and Hantao Mei (Southeast University, China)</i>	

## TrustCom-6: Security (V)

M-ETC: Improving Multi-Task Encrypted Traffic Classification by Reducing Inter-Task Interference .....	271
<i>Yuwei Xu (Southeast University, China; NSFOCUS Technologies Group Co., Ltd., China; Purple Mountain Laboratories for Network and Communication Security, China), Xiaotian Fang (Southeast University, China), Zhengxin Xu (Southeast University, China), Kehui Song (Tiangong University, China), Yali Yuan (Southeast University, China), and Guang Cheng (Southeast University, China; Purple Mountain Laboratories for Network and Communication Security, China)</i>	
Lattice-based Multi-Stage Secret Sharing 3D Secure Encryption Scheme .....	279
<i>Xu Li (Nanjing University of Aeronautics and Astronautics, China), Yinghao Wu (Nanjing University of Aeronautics and Astronautics, China), Yang Liu (Nanjing University of Aeronautics and Astronautics, China), Baosheng Wang (Nanjing University of Aeronautics and Astronautics, China), Bei Wang (Nanjing University of Aeronautics and Astronautics, China), and Yijun Cui (Nanjing University of Aeronautics and Astronautics, China)</i>	
Efficiently Detecting DDoS in Heterogeneous Networks: A Parameter-Compressed Vertical Federated Learning Approach .....	287
<i>Cao Chen (Institute of Information Engineering, Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China; Key Laboratory of Cyberspace Security Defense, China), Fenghua Li (Institute of Information Engineering, Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China; Key Laboratory of Cyberspace Security Defense, China), Yunchuan Guo (Institute of Information Engineering, Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China; Key Laboratory of Cyberspace Security Defense, China), Zifu Li (Institute of Information Engineering, Chinese Academy of Sciences, China; Key Laboratory of Cyberspace Security Defense, China), and Wenlong Kou (Institute of Information Engineering, Chinese Academy of Sciences, China; Key Laboratory of Cyberspace Security Defense, China)</i>	



Attack-Defense Graph Generation: Instantiating Incident Response Actions on Attack Graphs .....	295
<i>Kéren A. Saint-Hilaire (Polytechnique Montréal, Canada), Christopher Neal (Polytechnique Montréal, Canada), Frédéric Cuppens (Polytechnique Montréal, Canada), Nora Boulahia-Cuppens (Polytechnique Montréal, Canada), and Francesca Bassi (IRT SystemX, France)</i>	
SCENE: Shape-Based Clustering for Enhanced Noise-Resilient Encrypted Traffic Classification .....	306
<i>Meijie Du (Chinese Academy of Sciences; University of Chinese Academy of Sciences, China), Mingqi Hu (Chinese Academy of Sciences; University of Chinese Academy of Sciences, China), Shu Li (Chinese Academy of Sciences, China), Zhao Li (Chinese Academy of Sciences, China), and Qingyun Liu (Chinese Academy of Sciences, China)</i>	
GraySniffer: A Cliques Discovering Method for Illegal SIM Card Vendor Based on Multi-Source Data .....	316
<i>Tao Leng (Sichuan Police College, China), Chang You (Sichuan University, China), Shuangchun Luo (Sichuan University, China), Junyi Liu (Sichuan University, China), Yutong Zeng (Sichuan University, China), and Cheng Huang (Sichuan University, China)</i>	
 <b>TrustCom-7: Security (VI)</b>	
JASFREE: Grammar-Free Program Analysis for JavaScript Bytecode .....	326
<i>Hao Jiang (University of Science and Technology of China, China), Haiwei Lai (University of Science and Technology of China, China), Si Wu (University of Science and Technology of China, China), and Baojian Hua (University of Science and Technology of China, China)</i>	
SyntaxBridge: Protocol Description Transformer for Enhanced Formal Analysis of Security Protocols .....	338
<i>Liujia Cai (Information Engineering University, China), Tong Yu (Information Engineering University, China), Yumeng Li (Information Engineering University, China), Siqi Lu (Information Engineering University, China), Hanjie Dong (Hainan University, China; Zhengzhou University, China), Guangying Cai (Information Engineering University, China), Guangsong Li (Information Engineering University, China), and Yongjuan Wang (Information Engineering University, China)</i>	
STGCN-Based Link Flooding Attack Detection and Mitigation in Software-Defined Network .....	346
<i>Yue Li (Xidian University, China), Runcheng Fang (Xidian University, China), Qipeng Song (Xidian University, China), and Xilei Yang (Xidian University, China)</i>	

LayyerX: Unveiling the Hidden Layers of DoH Server via Differential Fingerprinting .....	354
<i>Yunyang Qin (Institute of Information Engineering, Chinese Academy of Sciences; University of Chinese Academy of Sciences, China), Yujia Zhu (Institute of Information Engineering, Chinese Academy of Sciences; University of Chinese Academy of Sciences, China), Linkang Zhang (Institute of Information Engineering, Chinese Academy of Sciences; University of Chinese Academy of Sciences, China), Baiyang Li (Institute of Information Engineering, Chinese Academy of Sciences; University of Chinese Academy of Sciences, China), Yong Ding (Institute of Information Engineering, Chinese Academy of Sciences; University of Chinese Academy of Sciences, China), and Qingyun Liu (Institute of Information Engineering, Chinese Academy of Sciences; University of Chinese Academy of Sciences, China)</i>	
WCDGA: BERT-Based and Character-Transforming Adversarial DGA with High Anti-Detection Ability .....	362
<i>Zhuji Guan (Southeast University, China), Mengmeng Tian (Southeast University, China), Yuwei Xu (Southeast University, China; Purple Mountain Laboratories for Network and Communication Security, China; Jiangsu Province Engineering Research Center of Security for Ubiquitous Network, China), Kehui Song (Jiangsu Province Engineering Research Center of Security for Ubiquitous Network, China; Tiangong University, China), and Guang Cheng (Southeast University, China; Purple Mountain Laboratories for Network and Communication Security, China; Jiangsu Province Engineering Research Center of Security for Ubiquitous Network, China)</i>	
Towards High-Quality Electromagnetic Leakage Acquisition in Side-Channel Analysis .....	370
<i>Xiaoran Huang (Nanjing University of Science and Technology, China), Yiwen Gao (Nanjing University of Science and Technology, China), Wei Cheng (LTCl, Télécom Paris, and Secure-IC S.A.S, France), Yuejun Liu (Nanjing University of Science and Technology, China), Jingdian Ming (Nanjing University of Science and Technology, China; Zhejiang University, China), Yongbin Zhou (Nanjing University of Science and Technology, China; Institute of Information Engineering, Chinese Academy of Sciences, China), and Jian Weng (Jinan University, China)</i>	

## **TrustCom-8: Security (VII)**

Cyber Risk Analysis on Electric Vehicle Systems via NIST CSF .....	378
<i>Spyridon Sourmelis (Technical University of Denmark, Denmark) and Weizhi Meng (Lancaster University, UK; Guangzhou University, China)</i>	
EUREKHA: Enhancing User Representation for Key Hackers Identification in Underground Forums .....	387
<i>Abdoul Nasser Hassane Amadou (University Mohammed VI Polytechnic, Morocco), Anas Motii (University Mohammed VI Polytechnic, Morocco), Saida Elouardi (University Mohammed VI Polytechnic, Morocco), and EL Houcine Bergou (University Mohammed VI Polytechnic, Morocco)</i>	

Few-Shot Encrypted Malicious Traffic Classification via Hierarchical Semantics and Adaptive Prototype Learning .....	399
<i>Yuan Zhao (Beihang University, China), Chunhe Xia (Beihang University, China; Guangxi Normal University, China), Tianbo Wang (Beihang University, China), Mengyao Liu (Beihang University, China), and Yang Li (Beihang University, China)</i>	
AIDE: Attack Inference Based on Heterogeneous Dependency Graphs with MITRE ATT&CK .....	410
<i>Weidong Zhou (Beihang University, China), Chunhe Xia (Beihang University, China; Guangxi Normal University, China), Nan Feng (Beihang University, China), Xinyi Pan (Peking University, China), Tianbo Wang (Beihang University, China), and Xiaojian Li (Guangxi Normal University, China)</i>	
From Scarcity to Clarity: Few-Shot Learning for DoH Tunnel Detection Through Prototypical Network .....	418
<i>Beibei Feng (Institute of Information Engineering, Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China), Qi Wang (National Computer Network Emergency Response Technical Team/Coordination Center of China, China), Xiaolin Xu (Zhongguancun Laboratory, China), Yijing Wang (Institute of Information Engineering, Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China), Tianning Zang (Institute of Information Engineering, Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China), and Jingrun Ma (Institute of Information Engineering, Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China)</i>	
SBOM Generation Tools in the Python Ecosystem: An In-Detail Analysis .....	427
<i>Serena Cofano (IMT Lucca &amp; University of Genoa, Italy), Giacomo Benedetti (University of Genoa, Italy), and Matteo Dell'Amico (University of Genoa, Italy)</i>	
Shapley-Value-Based Explanations for Cryptocurrency Blacklist Detection .....	435
<i>Feixue Yan (Swinburne University of Technology, Australia), Sheng Wen (Swinburne University of Technology, Australia), Yang Xiang (Swinburne University of Technology, Australia), and Shiping Chen (CSIRO's Data61, Australia)</i>	

## TrustCom-9: Privacy (I)

Controllable Quantum Computing Privacy via Inherent Noises and Quantum Error Mitigation .....	443
<i>Keyi Ju (Beijing University of Posts and Telecommunications, China), Hui Zhong (University of Houston, USA), Xinyue Zhang (Kennesaw State University, USA), Xiaoqi Qin (Beijing University of Posts and Telecommunications, China), and Miao Pan (University of Houston, USA)</i>	

Scalable Client-Side Encrypted Deduplication Beyond Secret Sharing of the Master Key .....	453
<i>Yuchen Chen (Nankai University, China; Tianjin Key Laboratory of Network and Data Security Technology, and DISSec, China), Guanxiong Ha (Nankai University, China; Tianjin Key Laboratory of Network and Data Security Technology, and DISSec, China), Xuan Shan (Nankai University, China; Tianjin Key Laboratory of Network and Data Security Technology, and DISSec, China), Chunfu Jia (Nankai University, China; Tianjin Key Laboratory of Network and Data Security Technology, and DISSec, China), and Qiaowen Jia (University of Chinese Academy of Sciences, China)</i>	
Machine Learning-Based Optimal Data Trading Mechanism with Randomized Privacy Protection Scheme .....	461
<i>Xiaohong Wu (Huzhou University, China), Yujun Lin (Huzhou University, China), Jie Tao (Huzhou University, China), and Yonggen Gu (Huzhou University, China)</i>	
You are as you Type: Investigating the Influence of Timestamp Accuracy on the Robustness of Keystroke Biometrics .....	469
<i>Florian Dehling (University of Giessen, Germany), Sebastian Koch (University of Giessen, Germany), Luigi Lo Iacono (University of Giessen, Germany), and Hannes Federrath (University of Hamburg, Germany)</i>	
Towards Privacy-Aware IoT Communications: Delegable, Revocable, and Efficient .....	481
<i>Pengfei Wu (Singapore Management University, Singapore), Jianfei Sun (Singapore Management University, Singapore), Guomin Yang (Singapore Management University, Singapore), and Robert H. Deng (Singapore Management University, Singapore)</i>	
TrustNotify: A Lightweight Framework for Complete and Trustworthy Data Deletion Notification Distribution .....	492
<i>Qipeng Song (Xidian University, China), Ruiyun Wang (Xidian University, China), Yue Li (Xidian University, China), Yiheng Yan (Xidian University, China), Xingyue Zhu (Xidian University, China), and Hui Li (Xidian University, China)</i>	

## **TrustCom-10: Privacy (II)**

Budget-Feasible Double Auction Mechanisms for Model Training Services in Federated Learning Market .....	501
<i>Ting Zhou (Shandong University, China), Hongtao Lv (Shandong University, China), Ning Liu (Shandong University, China), and Lei Liu (Shandong University, China; Shandong Research Institute of Industrial Technology, China)</i>	
VCaDID: Verifiable Credentials with Anonymous Decentralized Identities .....	508
<i>Yalan Wang (University of Surrey, UK), Liqun Chen (University of Surrey, UK), Long Meng (University of Surrey, UK), and Christopher J.P. Newton (University of Surrey, UK)</i>	

A Framework for Detecting Hidden Partners in App Collusion .....	516
<i>Qinchen Guan (Henan Key Laboratory of Cyberspace Situation Awareness, China), Shaoyong Du (Henan Key Laboratory of Cyberspace Situation Awareness, China; Ministry of Education, China), Kerong Wang (Henan Key Laboratory of Cyberspace Situation Awareness, China), Chunfang Yang (Henan Key Laboratory of Cyberspace Situation Awareness, China; Ministry of Education, China), and Xiangyang Luo (Henan Key Laboratory of Cyberspace Situation Awareness, China; Ministry of Education, China)</i>	
Enhancing Privacy-Preserving Multi-Authority Attribute-Based Encryption: Addressing Rogue-Key Attacks Under Adaptive Corruption of Authorities .....	524
<i>Jingchi Zhang (Nanyang Technological University, Singapore) and Anwitaman Datta (Nanyang Technological University, Singapore / De Montfort University, UK)</i>	
VDPSRQ: Achieving Verifiable and Dynamic Private Spatial Range Queries over Outsourced Database .....	532
<i>Haoyang Wang (Xidian University, China; Cryptograph and Cyber Security Whampo Institute, China), Kai Fan (Xidian University, China; Cryptograph and Cyber Security Whampo Institute, China), Yue Quan (Xidian University, China), Fenghua Li (Chinese Academy of Sciences, China), and Hui Li (Xidian University, China)</i>	
DPFCIL: Differentially Private Federated Class-Incremental Learning on Non-IID Data .....	542
<i>Fuyao Zhang (Xidian University, China), Dan Wang (Xidian University, China), and Chuyang Liang (China Satellite Network Exploration Co., Ltd., China)</i>	
<b>TrustCom-11: Privacy (III)</b>	
Secure Federated Learning Schemes Based on Multi-Key Homomorphic Encryption .....	551
<i>Wenxiu Ding (Xidian University, China), Hongjiang Guo (Xidian University, China), Zheng Yan (Xidian University, China), and Mingjun Wang (Xidian University, China)</i>	
TriViewNet: Achieve Accurate Tor Hidden Service Classification by Multi-View Feature Extraction and Fusion .....	559
<i>Yuwei Xu (Southeast University, China; Purple Mountain Laboratories for Network and Communication Security, China; Jiangsu Province Engineering Research Center of Security for Ubiquitous Network, China), Jiangfeng Li (Southeast University, China), Yujie Hou (Southeast university, China), Xinxu Huang (Southeast university, China), Yali Yuan (Southeast university, China; Jiangsu Province Engineering Research Center of Security for Ubiquitous Network, China), and Guang Cheng (Southeast university, China; Purple Mountain Laboratories for Network and Communication Security, China; Jiangsu Province Engineering Research Center of Security for Ubiquitous Network, China)</i>	
SP2-RD2D: Secure and Privacy-Preserving Authentication and Key Agreement Protocol for D2D Relay Communication .....	567
<i>Mingjun Wang (Xidian University, China), Yixuan Liu (Xidian University, China), and Wenxiu Ding (Xidian University, China)</i>	

Enhanced Privacy Policy Comprehension via Pre-Trained and Retrieval-Augmented Models .....	574
<i>Xin Zhang (University of Science and Technology of China, China), Bingbing Zhang (University of Science and Technology of China, China), Chi Zhang (University of Science and Technology of China, China), and Lingbo Wei (Hefei Comprehensive National Science Center, China)</i>	
MIND: A Privacy-Preserving Model Inference Framework via End-Cloud Collaboration .....	582
<i>Siyuan Guan (Xidian University, China), Ziheng Hu (Xidian University, China), Guotao Xu (Xidian University, China), Yao Zhu (Xidian University, China), and Bowen Zhao (Xidian University, China)</i>	
Analyzing Relationship Consistency in Digital Forensic Knowledge Graphs with Graph Learning .....	590
<i>Ruoyao Xiao (University of Missouri-Kansas City, USA), Yu Luo (University of Central Missouri, USA), Weifeng Xu (The University of Baltimore, USA), Harshmeet Lamba (University of Missouri-Kansas City, USA), and Dianxiang Xu (University of Missouri-Kansas City, USA)</i>	

## TrustCom-12: Emerging Tech (I)

TransFront: Bi-Path Feature Fusion for Detecting Front-Running Attack in Decentralized Finance .....	600
<i>Yuheng Zhang (Guangzhou University, China), Guojun Wang (Guangzhou University, China), Peiqiang Li (Guangzhou University, China), Xubin Li (Guangzhou University, China), Wanyi Gu (Guangzhou University, China), Mingfei Chen (Guangzhou University, China), and Houji Chen (Guangzhou University, China)</i>	
RAG-Based Cyber Threat Tracing Graph Modeling Method .....	608
<i>Jong-Hee Jeon (Sejong University, Republic of Korea), Jahoon Koo (Sejong University, Republic of Korea), and Young-Gab Kim (Sejong University, Republic of Korea)</i>	
AdaptFL: Adaptive Client Task Allocation-Based Synchronous Federated Learning .....	616
<i>Xiaoshuang Li (Xidian University, China), Mingjun Wang (Xidian University, China), Yilong Guo (Xidian University, China), and Wenxiu Ding (Xidian University, China)</i>	
TierFlow: A Pipelined Layered BFT Consensus Protocol for Large-Scale Blockchain .....	624
<i>Yongkang Yu (Beihang University, China), Jinchun He (Beihang University, China), Xinwei Xu (Beihang University, China), Qinnan Zhang (Beihang University, China), Wangjie Qiu (Beihang University, China; Zhongguancun Laboratory, China), Hongwei Zheng (Beihang University, China; Beijing Academy of Blockchain and Edge Computing(BABEC), China), Binghui Guo (Beihang University, China; Zhongguancun Laboratory, China), and Jin Dong (Beihang University, China; Beijing Academy of Blockchain and Edge Computing(BABEC), China)</i>	

ClusterX: Adaptive Collaborative Scheduling of Layered User-Proxy Mapping to Enhance DDoS Defense in Distributed Clusters .....	636
<i>Jianbo Lin (Beijing University of Posts and Telecommunications, China), Lin Yan (Beijing University of Posts and Telecommunications, China), Zhi Lin (Beijing University of Posts and Telecommunications, China), Zan Zhou (Beijing University of Posts and Telecommunications, China), and Shujie Yang (Beijing University of Posts and Telecommunications, China)</i>	
New Compact Construction of FHE from Cyclic Algebra LWE .....	643
<i>Yuan Liu (Nanjing University of Science and Technology, China), Licheng Wang (Beijing Institute of Technology, China), and Yongbin Zhou (Nanjing University of Science and Technology, China)</i>	

## TrustCom-13: Emerging Tech (II)

Rethinking Mutation Strategies in Fuzzing Smart Contracts .....	650
<i>Jingzhang Cao (Hebei University, China), Meng Wang (Hebei University, China), and Shenao Lin (Hebei University, China)</i>	
Towards a Robust Medical Record System: Integrating Logical Reasoning for Trustworthy Data Management .....	658
<i>Hanning Zhang (China Unicom (Hainan) Innovation Research Institute, China), Guansheng Wang (China Unicom (Hainan) Industrial Internet Co., Ltd, China), Junwei Feng (China Unicom (Hainan) Industrial Internet Co., Ltd, China), Lei Feng (China Unicom (Hainan) Industrial Internet Co., Ltd, China), Quan Gan (China United Network Communications Group Co., Ltd., China), and Long Ji (China Unicom (Hainan) Industrial Internet Co., Ltd, China)</i>	
CVchain: A Cross-Voting-Based Low Latency Parallel Chain System .....	666
<i>Jianrong Wang (Tianjin University, China), Yacong Ren (Tianjin University, China), Dengcheng Hu (Tianjin University, China), Qi Li (Tianjin University, China), Sen Li (Tianjin University, China), Xuewei Li (Tianjin University, China), and Xiulong Liu (Tianjin University, China)</i>	
A Novel Time Series Approach to Anomaly Detection and Correction for Complex Blockchain Transaction Networks .....	674
<i>Qi Xia (University of Electronic Science and Technology of China, China), Badjie Ansu (University of Electronic Science and Technology of China, China), Jianbin Gao (University of Electronic Science and Technology of China, China), Mupoyi Ntuala Grace (University of Electronic Science and Technology of China, China), Hu Xia (University of Electronic Science and Technology of China, China), and Obiri Isaac Amankona (University of Electronic Science and Technology of China, China)</i>	
A Sustainable Storage Compensation Method for Consortium Blockchain-Based Computing Power Trading .....	683
<i>Guangzhuo Zhu (Beijing University of Technology, China), Qian Wang (Beijing University of Technology, China), and Bei Gong (Beijing University of Technology, China)</i>	

A High-Accuracy Unknown Traffic Identification Method Based on Multi-View Contrastive Learning .....	691
<i>Yuwei Xu (Southeast University, China; NSFOCUS Technologies Group Co., Ltd.; Purple Mountain Laboratories for Network and Communication Security, China), Zizhi Zhu (Southeast University, China), Chufan Zhang (Southeast University, China), Kehui Song (Tiangong University, China), and Guang Cheng (Southeast University, China; Purple Mountain Laboratories for Network and Communication Security, China)</i>	

### **TrustCom-14: Emerging Tech (III)**

Attacking High-Order Masked Cryptosystem via Deep Learning-Based Side-Channel Analysis .....	699
<i>Zelong Zhang (Nanjing University of Science and Technology, China), Wei Cheng (Secure-IC S.A.S, France), Yongbin Zhou (Nanjing University of Science and Technology, China; Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China), Zehua Qiao (Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China), Yuhan Zhao (Nanjing University of Science and Technology, China), and Jian Weng (Jinan University, China)</i>	

Efficient and Accurate Min-Entropy Estimation Based on Decision Tree for Random Number Generators .....	707
<i>Yuan Ma (Key Laboratory of Cyberspace Security Defense, Institute of Information Engineering, CAS, China; School of Cyber Security, UCAS, China), Maosen Sun (Key Laboratory of Cyberspace Security Defense, Institute of Information Engineering, CAS, China; School of Cyber Security, UCAS, China), Wei Wang (Key Laboratory of Cyberspace Security Defense, Institute of Information Engineering, CAS, China), Tianyu Chen (Key Laboratory of Cyberspace Security Defense, Institute of Information Engineering, CAS, China; School of Cyber Security, UCAS, China), Na Lv (Key Laboratory of Cyberspace Security Defense, Institute of Information Engineering, CAS, China), and Dongchi Han (Key Laboratory of Cyberspace Security Defense, Institute of Information Engineering, CAS, China; School of Cyber Security, UCAS, China)</i>	

User Authentication Based on the Integration of Musical Signals and Ear Canal Acoustics .....	717
<i>Tongxi Chen (Technical University of Denmark, Denmark), Weizhi Meng (Technical University of Denmark, Denmark; Lancaster University, UK), and Wenjuan Li (The Education University of Hong Kong, China; Guangzhou University, China)</i>	

Multiplicative Masked M&M: An Attempt at Combined Countermeasures with Reduced Randomness .....	726
<i>Kaiyuan Li (The University of Electro-Communications, Japan), Haruka Hirata (The University of Electro-Communications, Japan), Daiki Miyahara (The University of Electro-Communications, Japan), Kazuo Sakiyama (The University of Electro-Communications, Japan), Yuko Hara (Institute of Science Tokyo, Japan), and Yang Li (The University of Electro-Communications, Japan)</i>	



Multi-Channel Leakage Detection Based on $X^2$ Test of Independence .....	734
<i>Xiaoyong Kou (Nanjing University of Science &amp; Technology, China), Wei Yang (Nanjing University of Science &amp; Technology, China), Peijin Cong (Nanjing University of Science &amp; Technology, China), and Gongxuan Zhang (Nanjing University of Science &amp; Technology, China)</i>	
MVSS: Blockchain Cross-Shard Account Migration Based on Multi-Version State Synchronization .....	742
<i>Weihan Wang (Tianjin University, China), Xiulong Liu (Tianjin University, China), Liyuan Ma (Tianjin University, China), Hao Xu (Tianjin University, China), GaoWei Shi (Tianjin University, China), Juncheng Ma (Tianjin University, China), and Keqiu Li (Tianjin University, China)</i>	
 <b>TrustCom-15: AI Trust (I)</b>	
Enhancing Adversarial Robustness through Self-Supervised Confidence-Based Denoising .....	750
<i>Yongkang Chen (Academy of Military Sciences, China), Tong Wang (Academy of Military Sciences, China), Wei Kong (Academy of Military Sciences, China), Taotao Gu (Academy of Military Sciences, China), Guiling Cao (Academy of Military Sciences, China), and Xiaohui Kuang (Academy of Military Sciences, China)</i>	
A Knowledge Graph Completion Method Based on Gated Adaptive Fusion and Conditional Generative Adversarial Networks .....	759
<i>Zhixuan Zhang (Hunan University of Technology, China), Yanhui Zhu (Hunan University of Technology, China), Yuezhong Wu (Hunan University of Technology, China), Fangteng Man (Hunan University of Technology, China), Hao Chen (Hunan University of Technology, China), and Xujian Ying (Hunan University of Technology, China)</i>	
MARS: Robustness Certification for Deep Network Intrusion Detectors via Multi-Order Adaptive Randomized Smoothing .....	767
<i>Mengdie Huang (Xidian University, China; Purdue University, USA), Yingjun Lin (Purdue University, USA), Xiaofeng Chen (Xidian University, China), and Elisa Bertino (Purdue University, USA)</i>	
GTree: GPU-Friendly Privacy-Preserving Decision Tree Training and Inference .....	775
<i>Qifan Wang (University of Auckland, New Zealand), Shujie Cui (Monash University, Australia), Lei Zhou (National University of Defense Technology, China), Ye Dong (Singapore University of Technology and Design, Singapore), Jianli Bai (Singapore Management University, Singapore), Yun Sing Koh (University of Auckland, New Zealand), and Giovanni Russello (University of Auckland, New Zealand)</i>	
RTS: A Training-Time Backdoor Defense Strategy Based on Weight Residual Tendency .....	786
<i>Fan Xiang (University of Chinese Academy of Sciences, China), Xueyang Li (University of Chinese Academy of Sciences, China), and Guozhu Meng (University of Chinese Academy of Sciences, China)</i>	
Trustworthiness and Path Regularity Based Contrastive Learning for Noisy Knowledge Graph Error Assertion Detection .....	794
<i>Zhuohan Ao (Southwest University, China), Yi Wang (Southwest University, China), Ying Wang (Southwest University, China), and Yu Zhan (Southwest University, China)</i>	

## TrustCom-16: AI Trust (II)

RPG-Diff: Precise Adversarial Defense Based on Regional Positioning Guidance .....	802
<i>Haotian Wang (Inner Mongolia University, China) and Jing Liu (Inner Mongolia University, China)</i>	
Toward Privacy-Preserving and Verifiable XGBoost Training for Horizontal Federated Learning .....	810
<i>Wei Xu (Xidian University, China), Hui Zhu (Xidian University, China), Chang Xiao (Xidian University, China), Fengwei Wang (Xidian University, China), Dengguo Feng (State Key Laboratory of Computer Science, China), and Hui Li (Xidian University, China)</i>	
Local Drift Correction and Attention Aggregation for Self-Organized Federated Learning .....	818
<i>Haiying Liu (Inner Mongolia University of Science and Technology, China), Ruichun Gu (Inner Mongolia University of Science and Technology, China), Jingyu Wang (Inner Mongolia University of Science and Technology, China), Xiaolin Zhang (Inner Mongolia University of Science and Technology, China), Bolin Zhang (Inner Mongolia University of Science and Technology, China), and Xuebao Li (Inner Mongolia University of Science and Technology, China)</i>	
Boosting Transferability of Adversarial Examples by Joint Training and Dual Feature Mixup .....	826
<i>Mengmeng Tang (Guangzhou University, China), Shuhong Chen (Guangzhou University, China; Swinburne University of Technology, Australia), Guojun Wang (Guangzhou University, China), Hanjun Li (Guangzhou University, China), Zhuyi Yao (Guangzhou University, China), and Sheng Wen (Swinburne University of Technology, Australia)</i>	
Federated Unlearning for Samples Based on Adaptive Gradient Ascent of Angles .....	834
<i>Ying Hua (Ocean University of China, China), Hui Xia (Ocean University of China, China), and Shuo Xu (Ocean University of China, China)</i>	
Membership Inference Attacks via Dynamic Adversarial Perturbations Reduction .....	842
<i>Zehua Ding (Guizhou University, China), Youliang Tian (Guizhou University, China), Guorong Wang (Guizhou University, China), Jinbo Xiong (Fujian Normal University, China), and Jianfeng Ma (Xidian University, China)</i>	

## TrustCom-17: AI Trust (III)

Defending Against Backdoor Attacks through Causality-Augmented Diffusion Models for Dataset Purification .....	850
<i>Yuefeng Lai (Fujian Normal University, China), Lizhao Wu (Fujian Normal University, China), Hui Lin (Fujian Normal University, China), and Xiaokang Zhou (Kansai University, Japan; RIKEN Center for AIP, Japan)</i>	

LLM4MDG: Leveraging Large Language Model to Construct Microservices Dependency Graph ...	859
<i>Jiekang Hu (Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China), Yakai Li (Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China), Zhaoxi Xiang (Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China), Luping Ma (Chinese Academy of Sciences, China), Xiaoqi Jia (Chinese Academy of Sciences, China), and Qingjia Huang (Chinese Academy of Sciences, China)</i>	
StrucTrans: Zero-Query Structural Adversarial Attack Transferred from Masked Autoencoders to Image Classifiers .....	870
<i>Yi Ji (The University of Tokyo, Japan) and Isao Echizen (National Institute of Informatics, Japan)</i>	
A GPU-Based Privacy-Preserving Machine Learning Acceleration Scheme .....	880
<i>Jie Hou (Shandong University, China), Zengrui Huang (Tianjin Navigation Instruments Research Institute, China), Zhiyong Zhang (Quang Cheng Laboratory, China), Wei Zhang (Shandong University, China), and Lei Ju (Shandong University, China)</i>	
A Low-Cost Black-Box Jailbreak Based on Custom Mapping Dictionary with Multi-Round Induction .....	888
<i>Feng Wu (University of Technology Sydney, Australia), Weiqi Wang (University of Technology Sydney, Australia), Youyang Qu (Commonwealth Scientific and Industrial Research Organization, Australia), and Shui Yu (University of Technology Sydney, Australia)</i>	
TTFL: Towards Trustworthy Federated Learning with Arm Confidential Computing .....	896
<i>Lizhi Sun (Nanjing University, China), Jingzhou Zhu (Nanjing University, China), Boyu Chang (Nanjing University, China), Yixin Xu (Nanjing University, China), Bo Yang (Nanjing University, China), Hao Wu (Nanjing University, China), Fengyuan Xu (Nanjing University, China), and Sheng Zhong (Nanjing University, China)</i>	

## TrustCom-18: AI Trust (IV)

Topic-Aware Sensitive Information Detection in Chinese Large Language Model .....	908
<i>Yalin Sun (Xidian University, China), Ruiying Lu (Xidian University, China), Kang Li (Xidian University, China), and Yu Zheng (Xidian University, China)</i>	
UNIRE: Secure Trajectory-User Linking Model Aggregation with Knowledge Transfer .....	916
<i>Jiezhen Tang (Xidian University, China), Hui Zhu (Xidian University, China), Yandong Zheng (Xidian University, China), Junpeng Zhang (Xidian University, China), Fengwei Wang (Xidian University, China), Jiaqi Zhao (Xidian University, China), and Hui Li (Xidian University, China)</i>	
Zephyr: A High-Performance Framework for Graph Attention Networks on Heterogeneous Data .	926
<i>Wenxiu Ding (Xidian University, China), Muzhi Liu (Xidian University, China), Yuxuan Cai (Xidian University, China), Mingxin Chen (Shanghai Jiao Tong University, China), Zheng Yan (Xidian University, China), and Mingjun Wang (Xidian University, China)</i>	

AS-FIBA: Adaptive Selective Frequency-Injection for Backdoor Attack on Deep Face Restoration .....	934
<i>Zhenbo Song (Nanjing University of Science and Technology, China), Wenhao Gao (Nanjing University of Science and Technology, China), Zhenyuan Zhang (Nanjing University of Science and Technology, China), and Jianfeng Lu (Nanjing University of Science and Technology, China)</i>	
CertRob: Detecting PDF Malware with Certified Adversarial Robustness via Randomization Smoothing .....	944
<i>Lijun Gao (Xidian University, China) and Zheng Yan (Xidian University, China)</i>	
Paa-Tee: A Practical Adversarial Attack on Thermal Infrared Detectors with Temperature and Pose Adaptability .....	952
<i>Zhangchi Zhao (Beijing Electronic Science and Technology Institute, China), Jianyi Zhang (Beijing Electronic Science and Technology Institute, China), Liqun Shan (University of Louisiana at Lafayette, USA), Ziyin Zhou (Beijing Electronic Science and Technology Institute, China), Kaiying Han (SWJTU-LEEDS Joint School Southwest Jiaotong University, China), and Xiali Hei (University of Louisiana at Lafayette, USA)</i>	

## TrustCom-19: Trust (II)

T-ABE: A Practical ABE Scheme to Provide Trustworthy Key Hosting on Untrustworthy Cloud ....	960
<i>Shuaishuai Chang (Key Laboratory of Cyberspace Security Defense; Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China), Yuzhe Li (Key Laboratory of Cyberspace Security Defense; Chinese Academy of Sciences, China), Jinchao Zhang (Key Laboratory of Cyberspace Security Defense; Chinese Academy of Sciences, China), and Bo Li (Key Laboratory of Cyberspace Security Defense; Chinese Academy of Sciences, China)</i>	
Three-Body Problem: An Empirical Study on Smartphone-Based TEEs, TEE-Based Apps, and Their Interactions .....	968
<i>Xianghui Dong (Beijing University of Technology, China), Yin Liu (Beijing University of Technology, China), and Xuejun Yu (Beijing University of Technology, China)</i>	
A Trust Model with Fitness-Based Clustering Scheme in FANETs .....	978
<i>Junqiao Gao (Wuhan University, China), Chaklam Cheong (Wuhan University, China), Mansi Zhang (Wuhan University, China), Yue Cao (Wuhan University, China), Tao Peng (Datang Interconnection Technology (Wuhan) Co., Ltd., China), and Shahbaz Pervez (Whitecliffe, New Zealand)</i>	
TWCF: Trust Weighted Collaborative Filtering Based on Quantitative Modeling of Trust .....	986
<i>Wenting Song (The University of Texas at Austin, USA) and K. Suzanne Barber (The University of Texas at Austin, USA)</i>	
Analyzing the Effectiveness of Image Preprocessing Defenses Under Runtime Constraints .....	994
<i>Niklas Bunzel (Fraunhofer SIT / ATHENE / TU Darmstadt, Germany) and Gerrit Klause (Fraunhofer SIT / ATHENE, Germany)</i>	

FedSGProx: Mitigating Data Heterogeneity and Isolated Nodes in Graph Federated Learning .....	1000
<i>Xutao Meng (Changchun University of Technology, China), Qingming Li (Zhejiang University, China), Yong Li (Changchun University of Technology, China), Li Zhou (Zhejiang Lab, China), and Xiaoran Yan (Zhejiang Lab, China)</i>	

## TrustCom-20: Security (VIII)

Designing Secret Embedding Scheme Based on Bitcoin Transactions Pattern Controlling .....	1007
<i>Zheng Feng (Beijing Information Science and Technology University, China), Chunyu Xing (Beijing Information Science and Technology University, China), and Chen Liang (Beijing Information Science and Technology University, China)</i>	
Perturbing Vulnerable Bytes in Packets to Generate Adversarial Samples Resisting DNN-Based Traffic Monitoring .....	1015
<i>Jie Cao (Southeast University, China; Queen's University, Canada), Zhengxin Xu (Southeast University, China), Yunpeng Bai (Southeast University, China), Yuwei Xu (Southeast University, China; Purple Mountain Laboratories for Network and Communication Security, China), Qiao Xiang (Xiamen University, China), and Guang Cheng (Southeast University, China; Purple Mountain Laboratories for Network and Communication Security, China)</i>	
Enabling Robust Android Malicious Packet Capturing and Detection via Android Kernel .....	1022
<i>Mingyang Li (University of Electronic Science and Technology of China, China), Weina Niu (University of Electronic Science and Technology of China, China), Xinglong Chen (Southwest China Research Institute of Electronic Equipment, China), Jiacheng Gong (University of Electronic Science and Technology of China, China), Kegang Hao (Southwest China Research Institute of Electronic Equipment, China), and Xiaosong Zhang (University of Electronic Science and Technology of China, China)</i>	
Signcryption Based on Elliptic Curve CL-PKC for Low Earth Orbit Satellite Security Networking .....	1029
<i>Meiling Chen (China Mobile Research Institute, China), Yuanyuan Yang (Xidian University, China), Sixu Guo (China Mobile Research Institute, China), Jin Cao (Xidian University, China), Haitao Du (China Mobile Research Institute, China), and Li Su (China Mobile Research Institute, China)</i>	
A Multi-Hop Reasoning Framework for Cyber Threat Intelligence Knowledge Graph .....	1037
<i>Kai Zhou (Xiangtan University, China), Yong Xie (Xiangtan University, China), and Xin Liu (Xiangtan University, China)</i>	
LSD Attack: Exploiting Inconsistencies between Design and Implementation of Ethereum Protocols .....	1045
<i>Chenyu Li (Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China), Xiu Zhang (Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China), Xueping Liang (Florida International University), and Xiaorui Gong (Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China)</i>	

## TrustCom-21: Security (IX)

Lightweight Leakage-Resilient Authenticated Key Exchange for Industrial Internet of Things .....	1051
<i>Wenxin Jia (Southwest University, China), Zheng Yang (Southwest University, China), and Zhiqiang Ma (Fujian Normal University, China)</i>	
ConfigKG: Identify Routing Security Issues from Configurations Based on Knowledge Graph .....	1060
<i>Pengfei Li (National University of Defense Technology, China), Yujing Liu (National University of Defense Technology, China), Jinshu Su (National University of Defense Technology, China; Academy of Military Science, China), and Bo Yu (National University of Defense Technology, China)</i>	
CaptchaSAM: Segment Anything in Text-Based Captchas .....	1070
<i>Yijun Wang (Shanghai Jiao Tong University, China), Ziyi Zhou (Shanghai Jiao Tong University, China), Weiqi Bai (Shanghai Jiao Tong University, China), Ruijie Zhao (Southeast University, China), and Xianwen Deng (Shanghai Jiao Tong University, China)</i>	
Tibetan Microblogging User Data Analysis and Topic Identification .....	1077
<i>Guixian Xu (Minzu University of China, China) and Wenhui Gao (Minzu University of China, China)</i>	
Security Enhancement of UAV Swarm Empowered Downlink Transmission with Integrated Sensing and Communication .....	1083
<i>Runze Dong (Air Force Engineering University, China), Buhong Wang (Air Force Engineering University, China), Jiang Weng (Air Force Engineering University, China), Kunrui Cao (National University of Defense Technology, China), Jiwei Tian (Air Force Engineering University, China), and Tianhao Cheng (Air Force Engineering University, China)</i>	
SimLog: System Log Anomaly Detection Method Based on Simhash .....	1090
<i>Weiping Wang (Central South University, China), Huijuan Wang (Central South University, China), Yulu Hong (Central South University, China), Chenyu Wang (Central South University, China), Hong Song (Central South University, China), and Shigeng Zhang (Central South University, China)</i>	

## TrustCom-22: Security (X)

FREDet: Fine-Grained Malicious Traffic Detection Based on Frequency Domain Features .....	1097
<i>Zekai Song (University of Chinese Academy of Sciences, China), Yunpeng Li (University of Chinese Academy of Sciences, China), Jian Qin (University of Chinese Academy of Sciences, China), Changzhi Zhao (University of Chinese Academy of Sciences, China), Dongxu Han (University of Chinese Academy of Sciences, China), and Yuling Liu (University of Chinese Academy of Sciences, China)</i>	

Android Malware Detection Technology Based on SC-ViT and Multi-Feature Fusion .....	1105
<i>Qiulong Yu (Beijing Electronic Science and Technology Institute, China), Zhiqiang Wang (Beijing Electronic Science and Technology Institute, China), Lei Ju (Beijing Electronic Science and Technology Institute, China), Sicheng Yuan (Beijing Electronic Science and Technology Institute, China), and Ying Zhang (Beijing Electronic Science and Technology Institute, China)</i>	
SBCM: Semantic-Driven Reverse Engineering Framework for Binary Code Modularization .....	1115
<i>Shuang Duan (Ministry of Education, China), Hui Shu (Ministry of Education, China), Zihan Sha (Ministry of Education, China), and Yuyao Huang (Ministry of Education, China)</i>	
A Multi-Blockchain Based Anonymous Cross-Domain Authentication Scheme for Industrial Internet of Things .....	1125
<i>Chengqi Hou (Jiangxi Normal University, China), Wei Yang (Jiangxi Normal University, China), Yu Wang (Chinese Academy of Sciences, China), Zhiming Zhang (Jiangxi Normal University, China), Shaolong Chen (Jiangxi Normal University, China), and Beibei Li (Sichuan University, China)</i>	
Deep Learning-Based DDoS Attack Detection Using Adversarial Optimization .....	1135
<i>Dahai Yu (Chang'an University, China), Jianming Cui (Chang'an University, China), Yungang Jia (Coordination Center of China, China), Peiguo Fu (Coordination Center of China, China), and Ming Liu (Coordination Center of China, China)</i>	
Security Assessment of Customizations in Android Smartwatch Firmware .....	1141
<i>Yifan Yu (Shandong University, China; Quan Cheng Laboratory, China), Ruoyan Lin (Shandong University, China; Quan Cheng Laboratory, China), Shuang Li (Shandong University, China; Quan Cheng Laboratory, China), Qinsheng Hou (Shandong University, China; Quan Cheng Laboratory, China), Peng Tang (Quan Cheng Laboratory, China; Shandong University, China), and Wenrui Diao (Quan Cheng Laboratory, China; Shandong University, China)</i>	

## **TrustCom-23: Security (XI)**

Sec-Reduce: Secure Reduction of Redundant and Similar Data for Cloud Storage Based on Zero-Knowledge Proof .....	1149
<i>Zhihuan Yang (University of South China, China), Wenlong Tian (University of South China, China; Nanyang Technology University, Singapore), Emma Zhang (Needham High School, USA), and Zhiyong Xu (Suffolk University, USA)</i>	
Private Data Aggregation Enabling Verifiable Multisubset Dynamic Billing in Smart Grids .....	1155
<i>Qian Yang (Zhejiang Sci-Tech University, China), Chen Wang (Zhejiang Sci-Tech University, China), Jian Shen (Zhejiang Sci-Tech University, China), Yi Li (Swinburne University of Technology, Australia), and Dengzhi Liu (Jiangsu Ocean University, China)</i>	
Custom Permission Misconfigurations in Android: A Large-Scale Security Analysis .....	1161
<i>Rui Li (Singapore Management University, Singapore), Wenrui Diao (Shandong University, China), and Debin Gao (Singapore Management University, Singapore)</i>	

Orchestrating Security Protection Resource for Space-Ground Integrated Networks .....	1171
<i>Dongbin Chen (Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China; Key Laboratory of Cyberspace Security Defense, China; East China Jiaotong University, China), Yunchuan Guo (Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China; Key Laboratory of Cyberspace Security Defense, China), Xiao Wang (Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China; Key Laboratory of Cyberspace Security Defense, China), Fenghua Li (Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China; Key Laboratory of Cyberspace Security Defense, China), and Zifu Li (Chinese Academy of Sciences, China; Key Laboratory of Cyberspace Security Defense, China)</i>	
Phase Shift Matrix Optimization and Channel Quantization Alternating in RIS-Assisted Physical Layer Key Generation .....	1179
<i>Liquan Chen (Southeast University, China), Yufan Song (Southeast University, China), Wanting Ma (Southeast University, China), Tianyu Lu (Southeast University, China), and Peng Zhang (Southeast University, China)</i>	
BWG: An IOC Identification Method for Imbalanced Threat Intelligence Datasets .....	1187
<i>Juncheng Lu (Southeast University, China), Yiyang Zhao (Southeast University, China), Yan Wang (Southeast University, China), Jiyuan Cui (Southeast University, China), and Sanfeng Zhang (Southeast University, China)</i>	

## **TrustCom-24: Security (XII)**

Network Traffic Anomaly Detection Method Based on CTA-BiLSTM .....	1195
<i>Wenlong Liu (Hainan Normal University, China), Bin Wen (Hainan Normal University, China), Mengshuai Ma (Hainan Normal University, China), and Wanrong Du (Hainan Normal University, China)</i>	
Decentralized and Lightweight Cross-Chain Transaction Scheme Based on Proxy Re-Signature ...	1201
<i>Huiying Zou (China University of Geosciences, China), Jia Duan (Hunan Engineering Research Center of Geographic Information Security and Application, China), Xi Liu (Hunan Engineering Research Center of Geographic Information Security and Application, China), Wei Ren (China University of Geosciences, China; Sichuan University, China; CASM, China), Tao Li (Sichuan University, China), Xianghan Zheng (Fuzhou University, China), and Kim-Kwang Raymond Choo (University of Texas at San Antonio, USA)</i>	
LLMUZZ: LLM-Based Seed Optimization for Black-Box Device Fuzzing .....	1209
<i>Guangming Gao (Jiangnan University, China), Shuitao Gan (Laboratory for Advanced Computing and Intelligence Engineering, China), Xiaofeng Wang (Pengcheng Laboratory, China), and Shengkai Zhu (Jiangnan University, China)</i>	
FCSec: An Open-Source Testbed for Security Evaluation on UAV Communications .....	1217
<i>Indu Chandran (K K Birla Goa Campus, India), Mukesh Narayana Gadde (K K Birla Goa Campus, India), and Kizheppatt Vipin (K K Birla Goa Campus, India)</i>	



Active Defense Research: A New Perspective Integrating Traps and Vulnerabilities .....	1225
<i>Quan Hong (University of Chinese Academy of Sciences, China; Chinese Academy of Sciences, China), Yang Yu (Tencent, China), Loyang Zhang (Chinese Academy of Sciences, China), and Lidong Zhai (Chinese Academy of Sciences, China)</i>	

Enhancing Graph-Based Vulnerability Detection through Standardized Deep Learning Pipelines. 1231
<i>Jiashun Hao (Kyungpook National University, South Korea) and Young-Woo Kwon (Kyungpook National University, South Korea)</i>

## TrustCom-25: Security (XIII)

OSN Bots Traffic Transformer : MAE-Based Multimodal Social Bots Behavior Pattern Mining .....	1239
<i>Haonan Zhai (Institute of Information Engineering, Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China), Ruiqi Liang (Institute of Information Engineering, Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China), Zhenzhen Li (Institute of Information Engineering, Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China), Zhen Li (Institute of Information Engineering, Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China), Wei Xia (Institute of Information Engineering, Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China), Bingxu Wang (Institute of Information Engineering, Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China), and Qingya Yang (Institute of Information Engineering, Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China)</i>	

Enhancing Higher-Order Masking: A Faster and Secure Implementation to Mitigate Bit Interaction Leakage .....	1247
<i>Jiahao Zhang (Nanjing University of Science and Technology, China), Yuejun Liu (Nanjing University of Science and Technology, China), Jingdian Ming (Nanjing University of Science and Technology, China; Zhejiang University, China), Yiwen Gao (Nanjing University of Science and Technology, China), Yongbin Zhou (Nanjing University of Science and Technology, China; Chinese Academy of Sciences, China), and Debao Wang (Nanjing University of Science and Technology, China)</i>	

Towards Securing ASCON Implementation by Inner Product Masking .....	1255
<i>Yuming Liu (Nanjing University of Science and Technology, China), Wei Cheng (Secure-IC S.A.S, France), Jihao Fan (Nanjing University of Science and Technology, China; Laboratory for Advanced Computing and Intelligence Engineering, China), and Yongbin Zhou (Nanjing University of Science and Technology, China; Chinese Academy of Sciences, China)</i>	

A Novel zk-SNARKs Method for Cross-Chain Transactions in Multi-Chain System .....	1261
<i>Pengcheng Xia (Nanjing University of Science and Technology, China), Jingyu Wu (Nanjing University of Science and Technology, China), Yiyang Ni (Jiangsu Second Normal University, China), and Jun Li (Nanjing University of Science and Technology, China)</i>	

LAPAID: A Lightweight, Adaptive and Perspicacious Active Intrusion Detection Method on Network Traffic Streams .....	1268
<i>Bin Li (National University of Defense Technology, China; Intelligent Game and Decision Lab (IGDL), China), Li Cheng (National University of Defense Technology, China), Zhongshan Zhang (National University of Defense Technology, China), Yu Pan (National University of Defense Technology, China), Feng Yao (National University of Defense Technology, China), and Renjie He (National University of Defense Technology, China)</i>	
WhisperMQTT: Lightweight Secure Communication Scheme for Subscription-Heavy MQTT Network .....	1276
<i>Youbin Kim (North Carolina State University, USA) and Man-Ki Yoon (North Carolina State University, USA)</i>	

## TrustCom-26: Security (XIV)

A Reliable Encrypted Traffic Classification Method Based on Attention Mechanisms .....	1286
<i>Zhijun Wu (Civil Aviation University of China, China), Shanhe Niu (Civil Aviation University of China, China), and Meng Yue (Civil Aviation University of China, China)</i>	
USB Catcher: Detection of Controlled Emissions via Conducted Compromising Emanations .....	1296
<i>Yixin Zhang (Institute of Information Engineering, Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China), Fuqiang Du (Institute of Information Engineering, Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China), Xinge Chi (Institute of Information Engineering, Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China), and Zhiqiang Lv (Institute of Information Engineering, Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China)</i>	
Improving Security in Internet of Medical Things through Hierarchical Cyberattacks Classification .....	1304
<i>Vince Noort (University College, Ireland), Nhien-An Le-Khac (University College, Ireland), and Hong-Hanh Nguyen-Le (University College, Ireland)</i>	
Privacy-Preserving Secure Neighbor Discovery for Wireless Networks .....	1310
<i>Ahmed Hussain (Networked Systems Security Group, KTH Royal Institute of Technology, Sweden) and Panos Papadimitratos (Networked Systems Security Group, KTH Royal Institute of Technology, Sweden)</i>	

D3IR: Securing Multi-Domain Networks via Extending Depth-in-Defense Strategies Across Nested Management Domains .....	1320
<i>Yaobing Xu (Institute of Information Engineering, Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China; Key Laboratory of Cyberspace Security Defense, China), Yunchuan Guo (Institute of Information Engineering, Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China; Key Laboratory of Cyberspace Security Defense, China), Wenlong Kou (Institute of Information Engineering, Chinese Academy of Sciences, China; Key Laboratory of Cyberspace Security Defense, China), Junhai Yang (Institute of Information Engineering, Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China; Key Laboratory of Cyberspace Security Defense, China), Ziyang Zhou (Institute of Information Engineering, Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China; Key Laboratory of Cyberspace Security Defense, China), and Fenghua Li (Institute of Information Engineering, Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China; Key Laboratory of Cyberspace Security Defense, China)</i>	
BGAS: Blockchain and Group Decentralized Identifiers Assisted Authentication Scheme for UAV Networks .....	1326
<i>Tingyu Wang (Beijing University of Posts and Telecommunications, China), Qiang Cao (Beijing University of Posts and Telecommunications, China), Shihong Zou (Beijing University of Posts and Telecommunications, China), and Yueming Lu (Beijing University of Posts and Telecommunications, China)</i>	

## TrustCom-27: Privacy (IV)

Sparse Silhouette Jump: Adversarial Attack Targeted at Binary Image for Gait Privacy Protection .....	1336
<i>Jiayi Li (Shanghai Jiao Tong University, China), Ke Xu (Shanghai Jiao Tong University, China), Xinghao Jiang (Shanghai Jiao Tong University, China), and Tanfeng Sun (Shanghai Jiao Tong University, China)</i>	
Real-Time Private Data Aggregation over Distributed Spatial-Temporal Infinite Streams with Local Differential Privacy .....	1343
<i>Xingxing Xiong (Jiangxi University of Finance and Economics, China), Shubo Liu (Wuhan University, China), Xiping Liu (Jiangxi University of Finance and Economics, China), Xiaoguang Niu (Wuhan University, China), and Wenyu You (Jiangxi University of Finance and Economics, China)</i>	
Enhancing IoT Privacy: Why DNS-Over-HTTPS Alone Falls Short? .....	1353
<i>Samuel Péliissier (University of Lyon, France), Gianluca Anselmi (University College London, UK), Abhishek Kumar Mishra (University of Lyon, France), Anna Maria Mandalari (University College London, UK), and Mathieu Cunche (University of Lyon, France)</i>	

Efficient FSS-Based Private Statistics for Traffic Monitoring .....	1361
<i>Zhichao Wang (Wuhan University, China), Qi Feng (Wuhan University, China), Min Luo (Wuhan University, China), Xiaolin Yang (Inspur Cloud Information Technology Co., Ltd., China), and Zizhong Wei (Inspur Cloud Information Technology Co., Ltd., China)</i>	
Efficient and Practical Multi-Party Private Set Intersection Cardinality Protocol .....	1371
<i>Shengzhe Meng (Tsinghua University, China), Xiaodong Wang (Tsinghua University, China), Zijie Lu (Beijing Institute of Mathematical Sciences and Applications, China), and Bei Liang (Beijing Institute of Mathematical Sciences and Applications, China)</i>	
An Efficient and Privacy-Preserving Participant Selection Scheme Based on Location in Mobile Crowdsensing .....	1381
<i>Yudan Cheng (Lanzhou University of Technology, China), Tao Feng (Lanzhou University of Technology, China), Zhiqian Liu (Jinan University, China), Xian Guo (Lanzhou University of Technology, China), Lulu Han (Luoyang Normal University, China), and Jianfeng Ma (Xidian University, China)</i>	

## **TrustCom-28: Privacy (V)**

NAGG: Noised Graph Node Feature Aggregations for Preserving Privacy .....	1389
<i>Yinghao Song (Data Intelligence Division, China Unicom Digital Technology Co., Ltd., China), Long Yan (Data Intelligence Division, China Unicom Digital Technology Co., Ltd., China), Yang Li (Data Intelligence Division, China Unicom Digital Technology Co., Ltd., China), Mingjian Ni (Peking University, China), Shengzhong Tan (Data Intelligence Division, China Unicom Digital Technology Co., Ltd., China), Dazhong Li (Data Intelligence Division, China Unicom Digital Technology Co., Ltd., China), Huiting Zhao (Data Intelligence Division, China Unicom Digital Technology Co., Ltd., China), and Yulun Song (Data Intelligence Division, China Unicom Digital Technology Co., Ltd., China)</i>	
EffiTaint: Boosting Sensitive Data Tracking with Accurate Taint Behavior Modeling and Efficient Access Path Optimization .....	1397
<i>Haocheng Li (Ocean University of China, China), Haipeng Qu (Ocean University of China, China), Gaozhou Wang (State Grid Shandong Electric Power, China), and Xiangjian Ge (Ocean University of China, China)</i>	
A Quiet Place: An In-Depth Study of Mobile Public-to-Private Attacks .....	1405
<i>Yin Liu (Beijing University of Technology, China)</i>	
Single-Sign-on Authentication with Anonymous Token and Restricted Covert Channel .....	1413
<i>Zhao Zhang (University of Electronic Science and Technology of China, China), Chunxiang Xu (University of Electronic Science and Technology of China, China), and Man Ho Allen Au (The Hong Kong Polytechnic University, Hong Kong Special Administrative Region of China)</i>	

DMASP: Dynamic Multi-Keyword Searchable Encryption for Protected Access and Search Patterns with Differential Privacy .....	1423
<i>Yue Quan (Xidian University, China; Cryptograph and Cyber Security Whampo Institute, China), Kai Fan (Xidian University, China; Cryptograph and Cyber Security Whampo Institute, China), Haoyang Wang (Xidian University, China), Hui Li (Xidian University, China), and Yintang Yang (Xidian University, China)</i>	

Research on Intelligent Joint Detection Technology for Application Privacy Behavior Compliance .....	1430
<i>Ruoding Zhang (University of Chinese Academy of Sciences, China), Tao Liu (Key Laboratory of Mobile Application Innovation and Governance Technology, MIIT, Chinese Academy of Information and Communications Technologies, China), Qifeng Shi (University of Chinese Academy of Sciences, China), Yan Zhang (University of Chinese Academy of Sciences, China), Xiaoyi Song (University of Chinese Academy of Sciences, China), and Xinrui Geng (Xi'an Jiaotong-Liverpool University, China)</i>	

## **TrustCom-29: Privacy (VI)**

Multi-Dimensional Data Collection Under Personalized Local Differential Privacy .....	1438
<i>Kunpeng Song (Shandong University, China; Quan Cheng Laboratory, China), Mingzhang Sun (Shandong University, China; Quan Cheng Laboratory, China), Kui Zhou (Shandong University, China), Peng Tang (Quan Cheng Laboratory, China; Shandong University, China), Ning Wang (Guangzhou University, China), and Shanqing Guo (Shandong University, China)</i>	

Interactive Verifiable Local Differential Privacy Protocols for Mean Estimation .....	1448
<i>Liang Wang (Shandong University, China; Quan Cheng Laboratory, China), Li Liu (Shandong University, China; Quan Cheng Laboratory, China), Pei Zhan (Shandong University, China; Quan Cheng Laboratory, China), Peng Tang (Quan Cheng Laboratory, China; Shandong University, China), Puwen Wei (Shandong University, China), and Shanqing Guo (Shandong University, China)</i>	

CFE: Secure Filtered Words in End-to-End Encrypted Messaging System .....	1458
<i>Tran Viet Xuan Phuong (University of Arkansas at Little Rock, USA), Albert Baker (University of Arkansas at Little Rock, USA), Philip Huff (University of Arkansas at Little Rock, USA), Jan P Springer (University of Arkansas at Little Rock, USA), and Tho Thi Ngoc Le (HUTECH University, Viet Nam)</i>	

Privacy-Preserving Multi-Soft Biometrics through Generative Adversarial Networks with Chaotic Encryption .....	1466
<i>Hongying Zheng (Chongqing University, China), Hongdie Li (Chongqing University, China), Di Xiao (Chongqing University, China), and Maolan Zhang (Chongqing University, China)</i>	

Data Privacy-Preserving and Communication Efficient Federated Multilinear Compressed Learning .....	1472
<i>Di Xiao (Chongqing University, China), Zhuyan Yang (Chongqing University, China), Maolan Zhang (Chongqing University, China), and Lvjun Chen (Chongqing University, China)</i>	

Secure Join and Compute in Encrypted Database .....	1480
<i>Tanusree Parbat (Indian Institute of Technology, India) and Ayantika Chatterjee (Indian Institute of Technology, India)</i>	

## TrustCom-30: Forensics and Analytics (I)

Dycom: A Dynamic Community Partitioning Technique for System Audit Logs .....	1486
<i>Zhaoyang Wang (Chinese Academy of Sciences; University of Chinese Academy of Sciences, China), Yanfei Hu (Academy of Mathematics and Systems Science, Chinese Academy of Sciences, China), Shuailou Li (Chinese Academy of Sciences; University of Chinese Academy of Sciences, China), Wenbo Wang (Chinese Academy of Sciences; University of Chinese Academy of Sciences, China), Lisong Zhang (Chinese Academy of Sciences; University of Chinese Academy of Sciences, China), Boyang Zhang (Chinese Academy of Sciences, China), Yu Wen (Chinese Academy of Sciences, China), and Dan Meng (Chinese Academy of Sciences, China)</i>	
Who Owns the Cloud Data? Exploring a Non-Interactive Way for Secure Proof of Ownership .....	1494
<i>Zhihuan Yang (University of South China, China), Wenlong Tian (University of South China, China; Nanyang Technology University, Singapore), Ruixuan Li (Huazhong University of Science and Technology, China), Xuming Ye (University of South China, China), and Zhiyong Xu (Suffolk University, USA)</i>	
Peering Through the Veil: A Segment-Based Approach for VPN Encapsulated Video Title Identification .....	1500
<i>Zhenyu Xu (Southeast University, China), Xurui Ren (Southeast University, China), Yi Zhang (Southeast University, China), Guang Cheng (Southeast University, China), and Hua Wu (Southeast University, China)</i>	
SecureNet-AWMI: Safeguarding Network with Optimal Feature Selection Algorithm .....	1506
<i>Ming Zhou (Nanjing University of Science and Technology, China), Zhijian Zheng (Nanjing University of Science and Technology, China), Peng Zhang (Nanjing University of Science and Technology, China), Sixue Lu (Shenyang Institute of Automation, CAS, China), Yamin Xie (University of Chinese Academy of Sciences, China), and Zhongfeng Jin (CNCERT/CC, China)</i>	
Unlocking Insights: An Extensible Framework for Automated Metadata Extraction from Online Documents .....	1512
<i>Raffaele Pizzolante (University of Salerno, Italy), Arcangelo Castiglione (University of Salerno, Italy), and Francesco Palmieri (University of Salerno, Italy)</i>	
Towards Understanding and Detecting File Types in Encrypted Files for Law Enforcement Applications .....	1522
<i>Adam L. Hooker (University of Texas at San Antonio, USA), Wenjian Huang (University of Texas at San Antonio, USA), Shalini Kapali (University of Texas at San Antonio, USA), Nishant Vishwamitra (University of Texas at San Antonio, USA), and Kim-Kwang Raymond Choo (University of Texas at San Antonio, USA)</i>	

## TrustCom-31: Emerging Tech (IV)

Broader but More Efficient: Broad Learning in Power Side-Channel Attacks .....	1528
<i>Yilin Yang (Wuhan University, China), Changhai Ou (Wuhan University, China), Yongzhuang Wei (Guilin University of Electronic Technology, China), Wei Li (Donghua University, China), Yifan Fan (Wuhan University, China), and Xuan Shen (National University of Defense Technology, China)</i>	
BedIDS: An Effective Network Anomaly Detection Method by Fusing Behavior Evolution Characteristics .....	1534
<i>Zhen Liu (Beijing Information Science &amp; Technology University, China), Chun Shan (Beijing Institute of Technology, China), Changzhen Hu (Beijing Institute of Technology, China), and Junkai Yi (Beijing Information Science &amp; Technology University, China)</i>	
Leveraging Large Language Models for Challenge Solving in Capture-the-Flag .....	1541
<i>Yuwen Zou (Xi'an Jiaotong-Liverpool University, China; University of Liverpool, UK), Yang Hong (Xi'an Jiaotong-Liverpool University, China), Jingyi Xu (Xi'an Jiaotong-Liverpool University, China), Lekun Liu (Xi'an Jiaotong-Liverpool University, China), and Wenjun Fan (Xi'an Jiaotong-Liverpool University, China)</i>	
Efficient and Verifiable Dynamic Skyline Queries in Blockchain Networks .....	1551
<i>Bo Yin (Changsha University of Science and Technology, China), Hang Chen (Changsha University of Science and Technology, China), Binyao Xu (Changsha University of Science and Technology, China), Mariam Suleiman Silima (Changsha University of Science and Technology, China), and Ke Gu (Changsha University of Science and Technology, China)</i>	
Enhancing Security and Privacy in Connected and Autonomous Vehicles: A Post-Quantum Revocable Ring Signature Approach .....	1557
<i>Qingmei Zhang (Xidian University, China; Qingdao University of Science and Technology, China), Pincan Zhao (Xidian University, China; Carleton University, Canada), Yuchuan Fu (Xidian University, China), and F. Richard Yu (Carleton University, Canada)</i>	
Leveraging Semi-Supervised Learning for Enhancing Anomaly-Based IDS in Automotive Ethernet .....	1563
<i>Jia Liu (Xi'an Jiaotong-Liverpool University, China; University of Liverpool, UK; Tsinghua University, P.R.China), Wenjun Fan (Xi'an Jiaotong-Liverpool University, China), Yifan Dai (Tsinghua University Suzhou Automotive Research Institute, P.R.China), Enggee Lim (Xi'an Jiaotong-Liverpool University, China), Zhoujin Pan (Tsinghua University Suzhou Automotive Research Institute, P.R.China), and Alexei Lisitsa (University of Liverpool, UK)</i>	

## TrustCom-32: Emerging Tech (V)

Robust Hardware Trojan Detection: Conventional Machine Learning vs. Graph Learning Approaches .....	1572
<i>Liang Hong (Northwestern Polytechnical University, China), Xingguo Guo (Northwestern Polytechnical University, China), Zeyar Aung (Khalifa University, UAE), and Wei Hu (Northwestern Polytechnical University, China)</i>	

UniTTP: A Unified Framework for Tactics, Techniques, and Procedures Mapping in Cyber Threats .....	1580
<i>Jie Zhang (Institute of Information Engineering, Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China), Hui Wen (Institute of Information Engineering, Chinese Academy of Sciences, China), Lun Li (Institute of Information Engineering, Chinese Academy of Sciences, China), and Hongsong Zhu (Institute of Information Engineering, Chinese Academy of Sciences, China)</i>	
HTV: Measuring Circuit Vulnerability to Hardware Trojan Insertion Based on Node Co-Activation Analysis .....	1589
<i>Shuiliang Chai (Zhejiang University of Technology, China), Zhanhui Shi (Zhejiang University of Technology, China), Yanjiao Gao (Zhejiang University of Technology, China), Yuhao Huang (Zhejiang University of Technology, China), Aizhu Liu (Zhejiang University of Technology, China), and Jie Xiao (Zhejiang University of Technology, China)</i>	
An Intelligent Affinity Strategy for Dynamic Task Scheduling in Cloud-Edge-End Collaboration .....	1595
<i>Jingsen Zhang (Beijing Information Science and Technology University, China), Shoulu Hou (Beijing Information Science and Technology University, China), Yi Gong (Beijing Information Science and Technology University, China), Tao Wang (Beijing Information Science and Technology University, China), Changyuan Lan (China Electronics Technology Group Corporation 27th Institute, China), and Xiulei Liu (Beijing Information Science and Technology University, China)</i>	
Hierarchical Graph Feature Extraction Based on Multi-Information Contract Graph for Enhanced Smart Contract Vulnerability Detection .....	1604
<i>Tao Fang (South China Normal University, China; Key Lab on Cloud Security and Assessment technology of Guangzhou, China), Zhihao Hou (South China Normal University, China; Key Lab on Cloud Security and Assessment technology of Guangzhou, China), Jiahao He (Webank Co., Ltd, China), Junjie Zhou (South China Normal University, China; Key Lab on Cloud Security and Assessment technology of Guangzhou, China), and Gansen Zhao (South China Normal University, China; Key Lab on Cloud Security and Assessment technology of Guangzhou, China)</i>	



LightRL-AD: A Lightweight Online Reinforcement Learning Approach for Autonomous Defense against Network Attacks .....	1614
---	------

*Fengyuan Shi (Institute of Information Engineering, Chinese Academy of Sciences; National Engineering Research Center of Information Security; University of Chinese Academy of Sciences, China), Zhou Zhou (Institute of Information Engineering, Chinese Academy of Sciences; National Engineering Research Center of Information Security, China), Jiang Guo (Institute of Information Engineering, Chinese Academy of Sciences; National Engineering Research Center of Information Security, China), Renjie Li (Institute of Information Engineering, Chinese Academy of Sciences; National Engineering Research Center of Information Security; University of Chinese Academy of Sciences, China), Zhongyi Zhang (Institute of Information Engineering, Chinese Academy of Sciences; National Engineering Research Center of Information Security; University of Chinese Academy of Sciences, China), Shu Li (Institute of Information Engineering, Chinese Academy of Sciences; National Engineering Research Center of Information Security, China), Qingyun Liu (Institute of Information Engineering, Chinese Academy of Sciences; National Engineering Research Center of Information Security, China), and Xiuguo Bao (National Computer Network Emergency Response Technical Team/Coordination Center of China, China)*

## TrustCom-33: Emerging Tech (VI)

SPDID: A Secure and Privacy-Preserving Decentralized Identity Utilizing Blockchain and PUF....	1622
--	------

*Yueyue He (Kyushu University, Japan), Wenxuan Fan (Kyushu University, Japan), and Koji Inoue (Kyushu University, Japan)*

Enhancing Security and Efficiency in Vehicle-to-Sensor Authentication: A Multi-Factor Approach with Cloud Assistance .....	1632
--	------

*Xinrui Zhang (Carleton University, Canada), Pincan Zhao (Xidian University, China; Carleton University, Canada), and Jason Jaskolka (Carleton University, Canada)*

AdvPurRec: Strengthening Network Intrusion Detection with Diffusion Model Reconstruction Against Adversarial Attacks .....	1638
--	------

*Nour Alhussien (Augusta University, USA) and Ahmed Aleroud (Augusta University, USA)*

Privacy Leak Detection in LLM Interactions with a User-Centric Approach .....	1647
---	------

*Tan Su (University of Science and Technology of China, China), Bingbing Zhang (University of Science and Technology of China, China), Chi Zhang (University of Science and Technology of China, China), and Lingbo Wei (University of Science and Technology of China, China)*

HFI: High-Frequency Component Injection Based Invisible Image Backdoor Attack .....	1653
---	------

*Huanlai Xing (Southwest Jiaotong University, China), Xuxu Li (Southwest Jiaotong University, China), Jing Song (Southwest Jiaotong University, China), Lexi Xu (Research Institute, China United Network Communications Corporation, China), Jincheng Peng (Southwest Jiaotong University, China), Bowen Zhao (Southwest Jiaotong University, China), and Li Feng (Southwest Jiaotong University, China)*

From Liberty to 1984: A Methodology for Systematically Deteriorating LLM Outputs through Habituation Tendencies .....	1659
<i>Dong Zhang (vivo Mobile Communication Co., Ltd., China), Zhiyuan Hu (vivo Mobile Communication Co., Ltd., China), Huijun Chen (vivo Mobile Communication Co., Ltd., China), Guangming Liu (vivo Mobile Communication Co., Ltd., China), Yinfeng Zheng (vivo Mobile Communication Co., Ltd., China), and Jinghui Lu (vivo Mobile Communication Co., Ltd., China)</i>	

## TrustCom-34: AI Trust (V)

Attack Data is Not Solely Paramount: A Universal Model Extraction Enhancement Method .....	1666
<i>Chuang Liang (Southeast University, China) and Jie Huang (Southeast University, China)</i>	
Active Source Inference Attack Based on Label-Flipping in Federated Learning .....	1675
<i>Lening Zhang (Ocean University of China, China) and Hui Xia (Ocean University of China, China)</i>	
A Universally Composable Key Management System Using Trusted Hardware .....	1681
<i>Zhenghao Lu (Shanghai Jiao Tong University, China), Ding Ma (Alibaba Group, China), Lei Fan (Shanghai Jiao Tong University, China), Xiuzhen Chen (Shanghai Jiao Tong University, China), Yongshuai Duan (Alibaba Group, China), and Jia Zhang (Alibaba Group, China)</i>	
Achieving Trusted GPU Allocation: An Empirical Study on Efficiency Changes of Deep Learning Training Tasks .....	1687
<i>Ziheng Zhang (Shandong University, China), Lei Liu (Shandong University, China; Shandong Research Institute of Industrial Technology, China), and Zhongmin Yan (Shandong University, China)</i>	
THEF: A Privacy-Preserving Framework for Transformer Inference Leveraging HE and TEE .....	1693
<i>Zehao Li (Shanghai Jiao Tong University, China; Nanhu Laboratory, China), Jiachun Liao (Nanhu Laboratory, China), Jinhao Yu (Nanhu Laboratory, China), and Lei Zhang (Nanhu Laboratory, China)</i>	
DMPA: A Compact and Effective Pipeline for Detecting Multiple Phishing Attacks .....	1701
<i>Xiaodong Huang (South China Normal University, China), Gangliang Li (South China Normal University, China), Chengfeng Chen (South China Normal University, China), and Shouqiang Liu (South China Normal University, China)</i>	

## TrustCom-35: AI Trust (VI)

Learning Robust and Repeatable Physical Camouflage for Aerial Object Detectors .....	1709
<i>Zilong He (Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China) and Hua Zhang (Chinese Academy of Sciences, China)</i>	

FedNIFW:Non-Interfering Fragmented Watermarking for Federated Deep Neural Network .....	1719
<i>Haiyu Deng (University of Technology Sydney (UTS), Australia), Xiaocui Dang (University of Technology Sydney (UTS), Australia), Yanna Jiang (University of Technology Sydney (UTS), Australia), Xu Wang (University of Technology Sydney (UTS), Australia), Guangsheng Yu (University of Technology Sydney (UTS), Australia), Wei Ni (University of Technology Sydney (UTS), Australia), and Ren Ping Liu (University of Technology Sydney (UTS), Australia)</i>	
An Effective Adversarial Text Attack through a Block-Sparse Approach with Hamiltonian Insights .....	1727
<i>Yaling Zhang (Xi'an University of Technology, China), Xiang Sun (Xi'an University of Technology, China), Yichuan Wang (Xi'an University of Technology, China), Dongtai Tang (Xi'an University of Technology, China), and Chen Zhao (Xi'an University of Technology, China)</i>	
End-to-End Speaker Anonymization Based on Location-Variable Convolution and Multi-Head Self-Attention .....	1733
<i>Feiyu Zhao (Tianjin University, China), Jianguo Wei (Tianjin University, China), Wenhuan Lu (Tianjin University, China), and Yongwei Li (Chinese Academy of Sciences, China)</i>	
DUDPA-TATD: A Lightweight Privacy-Preserving Anomaly Traffic Detection Method for Edge Computing Scenarios .....	1741
<i>Guanghan Li (Xinjiang University, China), Wenzhong Yang (Xinjiang University, China), Xiaodan Tian (Xinjiang University, China), and Jiaren Peng (Xinjiang University, China)</i>	
Defending Against Model Poisoning Attacks in Federated Learning via Client-Guided Trust .....	1749
<i>Xiangxiang Wang (Ocean University of China, China), Hui Xia (Ocean University of China, China), and Yingqi Zhang (Ocean University of China, China)</i>	

## **TrustCom-36: AI Trust (VII)**

Abstraction-Based Training for Robust Classification Models via Image Pixelation .....	1756
<i>Chen Yang (East China Normal University, China), Min Wu (East China Normal University, China), and Min Zhang (East China Normal University, China)</i>	
FusTP-FL: Enhancing Differential Federated Learning through Personalized Layers and Data Transformation .....	1762
<i>Xiong Yan (Nanjing University of Science and Technology, China), Kedong Yan (Nanjing University of Science and Technology, China), Chanying Huang (Nanjing University of Science &amp; Technology, China), Dan Yin (Beijing Univ. of Civil Engineering &amp; Architecture, China), and Shan Xiao (Fiberhome Comm. Tech. Co., China)</i>	
Large Language Model and Behaviour Tree Based Real-World Test Scenario Generation for Autonomous Vehicles .....	1770
<i>Yuliang Li (East China Normal University, China), Zhonglin Hou (East China Normal University, China; University of New South Wales, Australia), and Hong Liu (East China Normal University, China; Shanghai Uni-Sentry Intelligent Technology Co., Ltd, China)</i>	

Robust Purification Defense for Transfer Attacks Based on Probabilistic Scheduling Algorithm of Pre-Trained Models: A Model Difference Perspective .....	1776
<i>Xinlei Liu (Information Engineering University, China), Jichao Xie (Information Engineering University, China), Tao Hu (Information Engineering University, China), Hailong Ma (Information Engineering University, China; Ministry of Education, China), Baolin Li (Information Engineering University, China), Peng Yi (Information Engineering University, China; Ministry of Education, China), and Zhen Zhang (Information Engineering University, China)</i>	
Individual Fair Density-Peaks Clustering Based on Local Similar Center Graph and Similar Decision Matrix .....	1784
<i>Yiding Tang (Southwest University of Science and Technology, China), Zhijing Yang (Southwest University of Science and Technology, China), Yufan Peng (Southwest University of Science and Technology, China), and Hui Zhang (Southwest University of Science and Technology, China)</i>	
D <sup>2</sup> FL: Dimensional Disaster-Oriented Backdoor Attack Defense of Federated Learning .....	1790
<i>Yilong Li (Beijing Electronic Science and Technology Institute, China), Jianyi Zhang (Beijing Electronic Science and Technology Institute, China), Ziyin Zhou (Beijing Electronic Science and Technology Institute, China), Zezheng Sun (Beijing Electronic Science and Technology Institute, China), Xu Ji (Beijing Electronic Science and Technology Institute, China), Zeping Li (Beijing Electronic Science and Technology Institute, China), Jiameng Han (Beijing Electronic Science and Technology Institute, China), and Zhangchi Zhao (Beijing Electronic Science and Technology Institute, China)</i>	

## **The International Workshop on AI-Driven Trust, Security and Privacy in Computer Networks (AI-Driven TSP 2024)**

### **TrustCom-37:Trust (III)**

Improved Rectangle and Linear Attacks on Lightweight Block Cipher WARP .....	1797
<i>Yaxin Cui (Information Engineering University, China), Hong Xu (Information Engineering University, China), and Zhichao Xu (Information Engineering University, China)</i>	
SAMOC: Enabling Atomic Invocations for Cross-Chain Crowdsourcing Testing DApps in Industrial Control Through Trusted Smart Community and Lock Mechanism .....	1803
<i>Weiguo Huang (Guilin University of Electronic Technology, China), Yong Ding (Guilin University of Electronic Technology, China; HKCT Institute for Higher Education, China), Jun Li (China Industrial Control Systems Cyber Emergency Response Team, China), Yujue Wang (Hangzhou Innovation Institute of Beihang University, China), Hai Liang (Guilin University of Electronic Technology, China), and Changsong Yang (Guilin University of Electronic Technology, China; HKCT Institute for Higher Education, China)</i>	
Trustworthy Analysis of Drain3-Based Cold Storage Behavior in Judicial Depository Scenarios .....	1809
<i>Xiangyu Meng (Beijing University of Technology, China) and Xuejun Yu (Beijing University of Technology, China)</i>	

FCADD: Robust Watermarking Resisting JPEG Compression with Frequency Channel Attention and Distortion De-Gradient .....	1817
<i>Dong Yang (University of Science and Technology of China, China), Weihai Li (University of Science and Technology of China, China), Zikai Xu (University of Science and Technology of China, China), Zhiling Zhang (University of Science and Technology of China, China), and Yiling Chen (University of Science and Technology of China, China)</i>	
ASK-LTL Checker: A Tailored Model Checker for Linear Temporal Logic of CPN State Space .....	1825
<i>Jing Li (Inner Mongolia University, China), Tao Sun (Inner Mongolia University, China), and Wenjie Zhong (Inner Mongolia University, China)</i>	
Sustainable and Trusted Vehicular Energy Trading Enabled by Scalable Blockchains .....	1832
<i>Qingmei Yang (Qingdao University of Science and Technology, China; Xidian University, China), Ljun Sun (Qingdao University of Science and Technology, China), Xiao Chen (University of Leicester, UK), and Lingling Wang (Qingdao University of Science and Technology, China)</i>	

## TrustCom-38: Security (XV)

DyGCN: Dynamic Graph Convolution Network-Based Anomaly Network Traffic Detection .....	1838
<i>Yonghao Gu (Beijing University of Posts and Telecommunications, China), Xiaoqing Zhang (Beijing University of Posts and Telecommunications, China), Hao Xu (Beijing University of Posts and Telecommunications, China), and Tiejun Wu (Nsfocus Technologies Group Co. Ltd., China)</i>	
ROSE <sup>+</sup> : A Robustness-Optimized Security Scheme Against Cascading Failures in Multipath TCP under LDDoS Attack Streams .....	1844
<i>Jinquan Nie (Jiangxi Normal University, China), Lejun Li (Jiangxi Normal University, China), Yirui Jiang (School of Water, Energy, and Environment Cranfield University, UK), Young Ma (Jiangxi Normal University, China), and Yuanlong Cao (Jiangxi Normal University, China)</i>	
A Novel Approach to Network Traffic Analysis: the HERA Tool .....	1850
<i>Daniela Pinto (Polytechnic of Porto (ISEP-IPP), Portugal), Ivone Amorim (Polytechnic of Porto (IPP), Portugal), Eva Maia (Polytechnic of Porto (ISEP-IPP), Portugal), and Isabel Praça (Polytechnic of Porto (ISEP-IPP), Portugal)</i>	
Machine Learning-Based Power Allocation Optimization Algorithm for Enhanced CR-NOMA Network .....	1857
<i>Yu Fu (Dalian University of Technology, China), Bingcai Chen (Dalian University of Technology, China; Xinjiang Normal University, China), Qian Ning (Sichuan University, China), and Kai Lin (Dalian University of Technology, China)</i>	
A Self-Adaptive Framework for Responding to Uncertainty in Access Control Process with Deep Neural Networks .....	1863
<i>Jihoon Park (Sejong University, Republic of Korea), Giluk Kang (Sejong University, Republic of Korea), and Young-Gab Kim (Sejong University, Republic of Korea)</i>	

Efficient DDoS Detection and Mitigation in Cloud Data Centers Using eBPF and XDP .....	1869
<i>Ziyue Chen (Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China), He Kong (Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China), Shuai Ding (Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China), Quanfeng Lv (Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China), and Guo Wei (Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China)</i>	

## TrustCom-39: Security (XVI)

A LLM-Based Agent for the Automatic Generation and Generalization of IDS Rules .....	1875
<i>Xiaowei Hu (Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China), Haoning Chen (Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China), Huaifeng Bao (Tencent, China), Wen Wang (Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China), Feng Liu (Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China), Guoqiao Zhou (Chinese Academy of Sciences, China), and Peng Yin (University of Chinese Academy of Sciences, China; Defence Industry Secrecy Examination and Certification Center, China)</i>	

A Self-Supervised Targeted Process Anomaly Detection Method Based on the Minimum Set of Observed Events .....	1881
---	------

*Haojun Xia (Institute of Information Engineering, Chinese Academy of Sciences Beijing, China; University of Chinese Academy of Sciences Beijing, China), Limin Sun (Institute of Information Engineering, Chinese Academy of Sciences Beijing, China; University of Chinese Academy of Sciences Beijing, China), Wenliang Liu (State Grid Fujian Electric Power Co., Ltd, China), Jingyi Xie (State Grid Fujian Electric Power Co., Ltd, China), Zhanwei Song (Institute of Information Engineering, Chinese Academy of Sciences Beijing, China; University of Chinese Academy of Sciences Beijing, China), and Bibo Tu (Institute of Information Engineering, Chinese Academy of Sciences Beijing, China; University of Chinese Academy of Sciences Beijing, China)*

GeMuFuzz: Integrating Generative and Mutational Fuzzing with Deep Learning .....	1889
<i>Zheng Zhang (Beijing Institute of Technology, China), Rui Ma (Beijing Institute of Technology, China), Yuqi Zhai (Beijing Institute of Technology, China), Yuche Yang (Industrial and Commercial Bank of China), Siqi Zhao (Beijing Institute of Technology, China), and Hongming Chen (Beijing Institute of Technology, China)</i>	

A Cross-Site Scripting Attack Protection Framework Based on Managed Proxy .....	1896
<i>Cheng Tang (Purple Mountain Laboratories, China), Qingfeng Wang (National Digital Switching System Engineering &amp; Technological R&amp;D Center, China), Guozhen Cheng (National Digital Switching System Engineering &amp; Technological R&amp;D Center, China), Hao Liang (National Digital Switching System Engineering &amp; Technological R&amp;D Center, China), Jianhua Peng (Purple Mountain Laboratories, China), Meiyue Yang (Purple Mountain Laboratories, China), Wenyan Liu (National Digital Switching System Engineering &amp; Technological R&amp;D Center, China), Ming Liu (Purple Mountain Laboratories, China), and Lei Sha (Purple Mountain Laboratories, China)</i>	
IoT Device Fingerprinting from Periodic Traffic Using Locality-Sensitive Hashing .....	1904
<i>Jianhui Ming (Xinjiang University, China), Weiping Wang (Central South University, China), Linlin Zhang (Xinjiang University, China), Yingjie Hu (Central South University, China), and Shigeng Zhang (Central South University, China)</i>	
SGCML: Detecting Hacker Community Hidden in Chat Group .....	1910
<i>Tao Leng (Sichuan Police College, China), Junyi Liu (Sichuan University, China), Zhen Yang (Sichuan University, China), Chang You (Sichuan University, China), Yutong Zeng (Sichuan University, China), and Cheng Huang (Sichuan University, China)</i>	
 <b>TrustCom-40: Security (XVII)</b>	
DA-CPVD: Vulnerability Detection Method Based on Dual Attention Composite Pooling .....	1916
<i>Mengxuan Shi (Jiangsu University, China), Jinfu Chen (Jiangsu University, China), Saihua Cai (Jiangsu University, China), Ziyang Liu (Jiangsu University, China), and Jiapeng Zhou (Jiangsu University, China)</i>	
Cyber Resilience Framework for Web Server .....	1922
<i>Wanqiu Zhou (Information Engineering University, China; Purple Mountain Laboratories, China), Zheng Zhang (Information Engineering University, China), Yuan Yao (Purple Mountain Laboratories, China), Jiang Wang (Purple Mountain Laboratories, China), Jiaxin Ma (Information Engineering University, China; Purple Mountain Laboratories, China), and Hui Liu (Henan Normal University, China)</i>	
Improved Packet-Level Synthetic Network Traffic Generation .....	1928
<i>Jacob Soper (Queensland University of Technology, Australia), Yue Xu (Queensland University of Technology, Australia), Ernest Foo (Griffith University, Australia), Zahra Jadidi (Griffith University, Australia), and Kien Nguyen Thanh (Queensland University of Technology, Australia)</i>	
Exploring Permission Control Flaws in Mini-Apps .....	1935
<i>Jun Li (Boston University, USA), Yuting Zhang (Boston University, USA), Wu Zhou (Meta Platforms, USA), and Shengzhi Zhang (Boston University, USA)</i>	

Maldet: An Automated Malicious npm Package Detector Based on Behavior Characteristics and Attack Vectors .....	1942
<i>Yu Zhang (Ocean University of China, China), Haipeng Qu (Ocean University of China, China), Lingyun Ying (QI-ANXIN Technology Research Institute, China), and Linghui Wang (Ocean University of China, China)</i>	
An Adaptive Reputation Update Mechanism for Primary Nodes in PBFT .....	1948
<i>Limin Yu (University of Jinan, China), Yong Dong Wu (University of Jinan, China), Jiao Lu (University of Jinan, China), and Tong Li (University of Jinan, China)</i>	

## TrustCom-41: Security (XVIII)

Rabbit: Secure Encrypted Property Graph Search Scheme Supporting Data and Key Updates .....	1954
<i>Yingying Wu (Nanjing University of Science and Technology, China), Jiabei Wang (Nanjing University of Science and Technology, China), Dandan Xu (Nanjing University of Science and Technology, China), Yongbin Zhou (Nanjing University of Science and Technology, China; Chinese Academy of Sciences, China), and Yang Wang (Inspur Cloud Information Technology Co., Ltd, China)</i>	
Malware Traffic Classification Based on Multidimensional Features Learning .....	1963
<i>Yijie Huang (Southeast University, China), Wei Ding (Southeast University, China), and Mian Huang (Southeast University, China)</i>	
ADIoT : An Anomaly Detection Model for IoT Devices Based on Behavioral Feature Analysis .....	1972
<i>Liang Wang (Hebei University, China), Zhipeng Wang (Hebei University, China), and Meng Wang (Hebei University, China)</i>	
Detection of Sensitive Information Based on Transient Data in Store Buffer and Cache .....	1978
<i>Yan Chang (Shanxi Agricultural University, China), Yaqin Wu (Shanxi Agricultural University, China), Jianwu Rui (Chinese Academy of Sciences, China), Ming Cao (Beijing Kuaishou Technology Co, China), Yawei Yue (Shanxi Agricultural University, China), Yu Feng (Shanxi Agricultural University, China), Tingting He (Shanxi Agricultural University, China), Haihui Gao (Shanxi Agricultural University, China), and Zhen Lv (Shanxi Agricultural University, China)</i>	
Unsupervised Evaluation Method of Relative Coordination Degree from Group Perspective .....	1983
<i>Chenghan Zhang (Ministry of Education, China), Yan Liu (Ministry of Education, China), Daofu Gong (Ministry of Education, China), and Ling Wang (Ministry of Education, China)</i>	
DTAME: A Interpretable and Efficient Approach for ABAC Policy Mining and Evaluation Using Decision Trees .....	1989
<i>Zejun Lan (Beijing University of Posts and Telecommunications, China), Jianfeng Guan (Beijing University of Posts and Telecommunications, China), Xianming Gao (Institute of System Engineering, PLA Academy of Military Science, China), Tao Feng (Institute of System Engineering, PLA Academy of Military Science, China), Kexian Liu (Beijing University of Posts and Telecommunications, China), and Jianbang Chen (Beijing University of Posts and Telecommunications, China)</i>	



## TrustCom-42: Security (XIX)

- A Vulnerability Detection Method for Intermediate Code Based on a Relational Dependency Graph ..... 1998  
*Bing Xia (dept. ZhongYuan University of Technology, China), Chongjun Tang (dept. ZhongYuan University of Technology, China), Wenbo Liu (dept. ZhongYuan University of Technology, China), Shihao Chu (dept. ZhongYuan University of Technology, China), and Yu Dong (dept. ZhongYuan University of Technology, China)*
- SSC-IDS: A Robust In-Vehicle Intrusion Detection System Based on Self-Supervised Contrastive Learning ..... 2004  
*Zhuoqun Xia (Changsha University of Science and Technology, China), Yongbin Yu (Changsha University of Science and Technology, China), Jingjing Tan (Changsha University of Science and Technology, China), and Kejun Long (Hunan Key Laboratory of Smart Roadway and Cooperative Vehicle-Infrastructure Systems, China)*
- NLP and Neural Networks for Insider Threat Detection ..... 2010  
*Baghalizadeh-Moghadam Neda (Polytechnique Montreal, Canada), Neal Christopher (Polytechnique Montreal, Canada), Cuppens Frédéric (Polytechnique Montreal, Canada), and Boulahia-Cuppens Nora (Polytechnique Montreal, Canada)*
- Two-Stage Federated Learning Strategy for Fairness and Security in Vehicular Networks ..... 2019  
*Xin Zhang (Beijing Electronics Science and Technology Institute, China), Chao Guo (Chinese Academy of Sciences, China), and Buxin Guo (Beijing Electronics Science and Technology Institute, China)*
- 5G-PPDE: A Novel Adaptive Scaling Framework for Enhancing the Resilience of the 5G Cloud Core Network ..... 2025  
*Xinyu Huang (Southeast University, China), Xingxing Liao (Purple Mountain Laboratories, China), Jie Yang (National Digital Switching Engineering & Technological R&D Center, China), Wei You (National Digital Switching Engineering & Technological R&D Center, China), Wenhao Wu (Information Engineering University, China), Shiru Min (Southeast University, China), and Xinsheng Ji (National Digital Switching Engineering & Technological R&D Center, China)*
- Contextual Transformer-Based Node Embedding for Vulnerability Detection Using Graph Learning ..... 2031  
*Joseph Gear (Queensland University of Technology, Australia), Yue Xu (Queensland University of Technology, Australia), Ernest Foo (Griffith University, Australia), Praveen Gauravaram (Tata Consultancy Services, Research and Innovation, Australia), Zahra Jadidi (Griffith University, Australia), and Leonie Simpson (Queensland University of Technology, Australia)*

## TrustCom-43: Security (XX)

- CVALLM: A Cloud Platform Security Assessment Framework Based on Large Language Models 2039  
*Wangyuan Jing (University of Science and Technology of China, China), Chi Zhang (University of Science and Technology of China, China), Bingbing Zhang (University of Science and Technology of China, China), and Lingbo Wei (Institute of Dataspace Hefei Comprehensive National Science Center, China)*

Smart Contract-Based Auditing of Edge Data for Vehicular Networks .....	2045
<i>Yu Zhao (Changchun University of Science and Technology, China), Yangguang Tian (University of Surrey, China), Chunbo Wang (Changchun University of Science and Technology, China), Xiaoqiang Di (Changchun University of Science and Technology, China), and Hui Qi (Changchun University of Science and Technology, China)</i>	
FD-WF: A Multi-Tab Website Fingerprinting Attack Based on Fixed Dimensions for Tor Network	2051
<i>Ruizhe Zhang (Jiangsu University, China), Shangnan Yin (Jiangsu University, China), and Jinfu Chen (Jiangsu University, China)</i>	
Modelling GDPR-Compliance Based on Defeasible Logic Reasoning: Insights from Time Complexity Perspective .....	2060
<i>Naila Azam (University of Glasgow, UK), Alex Chak (University of Glasgow, UK), Anna Lito Michala (University of Glasgow, UK), Shuja Ansari (University of Glasgow, UK), and Nguyen Truong (University of Glasgow, UK)</i>	
A Blockchain-Based PHR Sharing Scheme with Attribute Privacy Protection .....	2068
<i>Chaohe Lu (Qufu Normal University, China), Zhongyuan Yu (Lanzhou University, China), Guijuan Wang (Qilu University of Technology (Shandong Academy of Sciences), China; Shandong Fundamental Research Center for Computer Science, China), Anming Dong (Qilu University of Technology (Shandong Academy of Sciences), China; Shandong Fundamental Research Center for Computer Science, China), and Xiang Tian (Qilu University of Technology (Shandong Academy of Sciences), China; Shandong Fundamental Research Center for Computer Science, China)</i>	
Secure Microwave QR Code Communication Using Pseudo-Random Constellation Rotation .....	2078
<i>Chunpeng Guo (Northwestern Polytechnical University, China), Beiyuan Liu (Northwestern Polytechnical University, China), Zeyang Sun (Harbin Institute of Technology, China), Chen Chen (KTH Royal Institute of Technology, Sweden), and Sai Xu (Northwestern Polytechnical University, China; Southeast University, China)</i>	

## **TrustCom-44: Privacy (VII)**

Federated Knowledge-Enhanced Graph Attention Network for Privacy-Preserving Social Recommendation .....	2084
<i>Xiaofei Hao (Hebei University, China), Liyuan Liu (Hebei University, China), Yimeng Wang (Hebei University, China), Fengyu Li (Hebei University, China), and Wanqing Wu (Hebei University, China)</i>	
Federated Learning Greedy Aggregation Optimization for Non-Independently Identically Distributed Data .....	2090
<i>Bosong Zhang (Northwest University, China), Qian Sun (Northwest University, China), Hai Wang (Northwest University, China), Linna Zhang (Northwest University, China), and Danyang Li (Northwest University, China)</i>	

Efficient Multi-Subset Fine-Grained Authorization PSI over Outsourced Encrypted Datasets .....	2098
<i>Jinlong Zheng (Dongguan University of Technology, China), Jia-Nan Liu (Dongguan University of Technology, China), Minhua Su (Dongguan University of Technology, China), Dingcheng Li (Dongguan University of Technology, China), Kai He (Dongguan University of Technology, China), and Xueqiao Liu (University of Wollongong, Australia)</i>	
A Federated Learning Scheme with Adaptive Hierarchical Protection and Multiple Aggregation..	2106
<i>Zhiqiang Wang (Beijing Electronic Science and Technology Institute, China; State Information Center, China), Xinyue Yu (Beijing Electronic Science and Technology Institute, China), and Ziqing Tian (Beijing Electronic Science and Technology Institute, China)</i>	
A Dual Defense Design Against Data Poisoning Attacks in Deep Learning-Based Recommendation Systems .....	2115
<i>Xiaocui Dang (University of Technology Sydney, Australia), Priyadarsi Nanda (University of Technology Sydney, Australia), Manoranjan Mohanty (Carnegie Mellon University, Qatar), and Haiyu Deng (University of Technology Sydney, Australia)</i>	
scE(match): Privacy-Preserving Cluster Matching of Single-Cell Data .....	2123
<i>Johannes Lohmöller (RWTH Aachen University, Germany), Jannis Scheiber (RWTH Aachen University, Germany), Rafael Kramann (RWTH Aachen University Hospital, Germany), Klaus Wehrle (RWTH Aachen University, Germany), Sikander Hayat (RWTH Aachen University Hospital, Germany), and Jan Pennekamp (RWTH Aachen University, Germany; RWTH Aachen University Hospital, Germany)</i>	
 <b>TrustCom-45: Privacy (VIII)</b>	
Block-Feature Fusion for Privacy-Protected Iris Recognition .....	2133
<i>Wiraj Udara Wickramaarachchi (Wuhan University of Technology, China; Rajarata University of Sri Lanka, Sri Lanka), Junwei Zhou (Wuhan University of Technology, China), Dongdong Zhao (Wuhan University of Technology, China), and Jianwen Xiang (Wuhan University of Technology, China)</i>	
CFB-DSSE: Efficient Secure Dynamic Searchable Encryption Scheme with Conjunctive Search for Smart Healthcare .....	2142
<i>Ruiwei Hou (Northeastern University, China), Fucui Zhou (Northeastern University, China), Zongye Zhang (Northeastern University, China), Jiacheng Li (Northeastern University, China), and Chongyang Wang (Northeastern University, China)</i>	
An Efficient and Secure Anonymous Query Protocol .....	2151
<i>Wenjo Hu (Dongguan University of Technology, China) and Yin Li (Dongguan University of Technology, China)</i>	
Privacy-Aware Data Aggregation Using Functional Encryption .....	2159
<i>Sehrish Shafeeq (Universität Hamburg, Germany) and Mathias Fischer (Universität Hamburg, Germany)</i>	

Evaluating Web-Based Privacy Controls: A User Study on Expectations and Preferences .....	2169
<i>Yuemeng Yin (University of New South Wales, Australia), Rahat Masood (University of New South Wales, Australia), Suranga Seneviratne (University of Sydney, Australia), and Aruna Seneviratne (University of New South Wales, Australia)</i>	

High-Capacity and High-Security Data Hiding in Encrypted Image Using Image Filtering and Image Blocking .....	2175
<i>Yanpeng Xiang (Southwest University, China), Tao Zhang (Southwest University, China), Jiahao Liu (Southwest University, China), Xinbo Zhang (Southwest University, China), and Yu Zhang (Southwest University, China)</i>	

## TrustCom-46: Privacy (IX)

Cross-Platform Network User Alignment Interference Methods Based on Obfuscation Strategy ...	2185
<i>Luyao Wang (Henan Key Laboratory of Cyberspace Situation Awareness, China), Yan Liu (Henan Key Laboratory of Cyberspace Situation Awareness, China), Xiaoyu Guo (Henan Key Laboratory of Cyberspace Situation Awareness, China), Ziqi Long (Henan Key Laboratory of Cyberspace Situation Awareness, China), and Chunfang Yang (Henan Key Laboratory of Cyberspace Situation Awareness, China)</i>	

Research on Toxic Speech Detection Based on Large Language Models .....	2191
<i>Weihaoli Li (Inner Mongolia University of Science &amp; Technology, China), Yongbing Gao (Inner Mongolia University of Science &amp; Technology, China), Yu Zhang (Inner Mongolia University of Science &amp; Technology, China), Lidong Yang (Inner Mongolia University of Science &amp; Technology, China), and Ruiping Gao (Baotou Public Security Bureau, China)</i>	

ZKFDT: A Fair Exchange Scheme for Data Trading Based on Efficient Zero-Knowledge Proofs ....	2197
<i>Jianwei Liu (Computer Network Information Center, Chinese Academy of Sciences, China), Wei Wan (Computer Network Information Center, Chinese Academy of Sciences, China), Chun Long (Computer Network Information Center, Chinese Academy of Sciences, China), Jing Li (Computer Network Information Center, Chinese Academy of Sciences, China), Fan Yang (Computer Network Information Center, Chinese Academy of Sciences, China), and Yuhao Fu (Computer Network Information Center, Chinese Academy of Sciences, China)</i>	

Dynamic Differential Privacy in Hierarchical Federated Learning: A Layerwise Adaptive Framework .....	2207
<i>Zhongyuan Qin (Southeast University, China), Dinglian Wang (Southeast University, China), and Minghua Wang (Southeast University, China)</i>	

OHSS: Optimizing Homomorphic Secret Sharing to Support Fast Matrix Multiplication .....	2213
<i>Shuguang Zhang (Chengfang Financial Technology Co., China), Jianli Bai (Singapore Management University, Singapore), Kun Tu (Chengfang Financial Technology Co., China), Ziyue Yin (New York University, USA), and Chan Liu (Shenyang Normal University, China)</i>	

A Method for Quantitative Object De-Identification Analysis of Anonymized Video .....	2221
<i>Deok-Han Kim (Sejong University, Republic of Korea), Yujun Kim (Sejong University, Republic of Korea), and Young-Gab Kim (Sejong University, Republic of Korea)</i>	

Witness Encryption Based on the SAT Problem .....	2227
<i>Xingbo Wang (Guilin University of Electronic Technology, China), Yuzhu Wang (Guilin University of Electronic Technology, China), and Mingwu Zhang (Guilin University of Electronic Technology, Hubei University of Technology, China)</i>	

## **TrustCom-47: Forensics and Analytics (II)**

Research on Adaptive Attention Dense Network Structure in Camera Source Recognition Method .....	2238
<i>HaoXuan Wu (Hunan University of Technology, China) and Zhiqiang Wen (Hunan University of Technology, China)</i>	

Compressed Video Action Recognition Based on Neural Video Compression .....	2244
<i>Yuting Mou (Shanghai Jiao Tong University, China), Ke Xu (Shanghai Jiao Tong University, China), Xinghao Jiang (Shanghai Jiao Tong University, China), and Tanfeng Sun (Shanghai Jiao Tong University, China)</i>	

Construction of Cyber-Attack Attribution Framework Based on LLM .....	2250
<i>Jingye Zhang (National University of Defense Technology, China), Ken Cheng (National University of Defense Technology, China), Xinli Xiong (National University of Defense Technology, China), Rongcheng Dong (National University of Defense Technology, China), Jun Huang (National University of Defense Technology, China), and She Jie (National University of Defense Technology, China)</i>	

Discriminating Malware Families Using Partitional Clustering .....	2256
<i>Pooja Mishra (Federation University Australia, Australia), Paul Black (Federation University Australia, Australia), Adil Bagirov (Federation University Australia, Australia), and Paul Pang (Federation University Australia, Australia)</i>	

Investigating Patterns of Adversarial Techniques for Cyberattack Forensics .....	2262
<i>Liming Lu (Singapore Institute of Technology, Singapore), Zhenlin Yu (Singapore Institute of Technology, Singapore), Peter Loh Kok Keong (Singapore Institute of Technology, Singapore), and Tuhin Isfaque AL Kaderi (Singapore Institute of Technology, Singapore)</i>	

WAPITI - A Weighted Bayesian Method for Private Information Inference on Social Ego Networks .....	2269
<i>Simo Hervois (Fraunhofer SIT, Germany) and Kreutzer Kreutzer (Fraunhofer SIT, Germany)</i>	

## TrustCom-48: Emerging Tech (VII)

DI-GAE: A Dynamic and Resource-Efficient Attack Detection Framework with Incremental Learning and Graph Autoencoders .....	2281
<i>Mengmi Tan (Beijing University of Posts and Telecommunications, China), Jianyi Liu (Beijing University of Posts and Telecommunications, China), and Ru Zhang (Beijing University of Posts and Telecommunications, China)</i>	
Transfer Learning-Based Robust Insider Threat Detection .....	2287
<i>Yujun Kim (Sejong University, Republic of Korea), Deok-Han Kim (Sejong University, Republic of Korea), and Young-Gab Kim (Sejong University, Republic of Korea)</i>	
Model-Based Data Markets: A Multi-Broker Game Theoretic Approach .....	2293
<i>Yizhou Ma (University of Southampton, UK), Xikun Jiang (University of Copenhagen, Denmark), Evan W. Wu (University of Southampton, UK), Luis-Daniel Ibáñez (University of Southampton, UK), and Jian Shi (University of Southampton, UK)</i>	
DcChain: A Novel Blockchain Sharding Method Based on Dual-Constraint Label Propagating ....	2302
<i>Hao Zhou (Nanjing University of Science and Technology, China), Pengcheng Xia (Nanjing University of Science and Technology, China), Yiyang Ni (Jiangsu Second Normal University, China), and Jun Li (Nanjing University of Science and Technology, China)</i>	
An Intelligent Charging Service Selection Scheme Under the Cross-Area Consensus of Blockchain for the IoV .....	2310
<i>Shuming Xiong (Jiangsu University, China; Jiangsu Province Key Laboratory of Security Technology for Industrial Cyberspace, China), Junfeng Zhu (Jiangsu University, China), and Qiqi Xu (Jiangsu University, China)</i>	
FlexiContracts: A Novel and Efficient Scheme for Upgrading Smart Contracts in Ethereum Blockchain .....	2316
<i>Md Tahrir Hossain (Syracuse University, USA), Sakib Hassan (University of Dhaka, Bangladesh), Faisal Haque Bappy (Syracuse University, USA), Muhammad Nur Yanhaona (BRAC University, Bangladesh), Sarker Ahmed Rume (University of Dhaka, Bangladesh), Moinul Zaber (University of Dhaka, Bangladesh; United Nations University, Portugal), and Tariqul Islam (Syracuse University, USA)</i>	

## TrustCom-49: AI Trust (VIII)

Fedfair: A Debiasing Algorithm for Federated Learning Systems .....	2322
<i>Haibin Zheng (Zhejiang University of Technology, China), Tianxin Zhang (Zhejiang University of Technology, China), and Jinyin Chen (Zhejiang University of Technology, China)</i>	
Differentially Private Graph Convolutional Networks with Privacy Amplification .....	2327
<i>Yifan Sun (University of Birmingham, UK) and Meng Song (Beihang University, China)</i>	

Destruction and Reconstruction Chain: An Adaptive Adversarial Purification Framework .....	2336
<i>Zeshan Pang (National University of Defense Technology, China), Shasha Guo (National University of Defense Technology, China), Xuehu Yan (National University of Defense Technology, China), and Yuliang Lu (National University of Defense Technology, China)</i>	
CNN-KOA-BiGRU: A High-Accuracy APT Detection Model Based on Deep Learning Networks .	2342
<i>Chaoqin Zhang (Zhengzhou University of Light Industry, China), Maoqi Sun (Zhengzhou University of Light Industry, China), and Guangwu Hu (Shenzhen Institute of Information Technology, China)</i>	
Efficient and Secure Federated Learning via Enhanced Quantization and Encryption .....	2348
<i>Chengming Zhang (Data Intelligent Platform System Department, ZTE Corporation, China), Bo Tang (Data Intelligent Platform System Department, ZTE Corporation, China), Yifan Bian (Data Intelligent Platform System Department, ZTE Corporation, China), Bingtao Han (Data Intelligent Platform System Department, ZTE Corporation, China), Yongcheng Wang (Data Intelligent Platform System Department, ZTE Corporation, China), and Tao Liu (Data Intelligent Platform System Department, ZTE Corporation, China)</i>	
Human Action Recognition by Invisible Sensing with the Constraint of Privacy Preservation .....	2354
<i>Jun Guo (Northwest University, China), Minjuan Sun (Northwest University, China), Weiwei Zhang (Xian Siyuan University, China), Baoying Liu (Northwest University, China), Anwen Wang (Northwest University, China), and Li Liu (Northwest University, China)</i>	

## **TrustCom-50: AI Trust (IX)**

Traceable AI-Driven Avatars Using Multi-Factors of Physical World and Metaverse .....	2360
<i>Kedi Yang (Guizhou University, China), Zhenyong Zhang (Guizhou University, China), and Youliang Tian (Guizhou University, China)</i>	
DDF-Net: A Cloud Computing Load Forecasting Method Integrating Spatiotemporal and Time-Frequency Domain Information .....	2368
<i>Yingjian Li (Inner Mongolia University of Technology, China), Yongsheng Wang (Inner Mongolia University of Technology, China), and Gang Wang (Inner Mongolia University of Technology, China)</i>	
HFL-AD: A Hierarchical Federated Learning Framework for Solving Data Contamination in DDoS Detection .....	2376
<i>Haishi Huang (Shanghai Jiao Tong University, China), Jiaping Gui (Shanghai Jiao Tong University, China), Jianan Hong (Shanghai Jiao Tong University, China), and Cunqing Hua (Shanghai Jiao Tong University, China)</i>	
Detectable Mislabeling - Can Faulty AI Models be Recognized from Incomplete Memory Traces?.	2382
<i>Łukasz Krzywiecki (Wrocław University of Science and Technology, Poland), Tadeusz Kulczycki (Wrocław University of Science and Technology, Poland), Christian Emmanuel Nteranya (Robert BOSCH SP. Z O.O., Poland), and Andrzej Stos (Université Clermont Auvergne and CNRS, France)</i>	

Privacy-Preserving Real-Time Gesture Recognition Using Cloud-Trained Neural Networks .....	2388
<i>Kewin Ignasiak (Wroclaw University of Science and Technology, Poland), Wojciech Kowalczyk (Wroclaw University of Science and Technology, Poland), Łukasz Krzywiecki (Wroclaw University of Science and Technology, Poland), Mateusz Nasewicz (Wroclaw University of Science and Technology, Poland), Hannes Salin (Swedish Transport Administration, Sweden), and Marcin Zawada (Wroclaw University of Science and Technology, Poland)</i>	
A Lightweight Privacy-Preserving and Verifiable Federated Learning-Based Protocol .....	2394
<i>Jiaqi Lei (Changsha University of Science and Technology, China), Ke Gu (Changsha University of Science and Technology, China), and Long Cai (Changsha University of Science and Technology, China)</i>	

## **TrustCom-51: AI Trust (X)**

BIG: A Practical Framework for Balancing the Conflict Between Group and Individual Fairness in Graph Neural Networks .....	2400
<i>Kuan Yan (The University of Sydney, Australia), Dmytro Matsypura (The University of Sydney, Australia), and Junbin Gao (The University of Sydney, Australia)</i>	
EasyDetector: Using Linear Probe to Detect the Provenance of Large Language Models .....	2410
<i>Jie Zhang (Institute of Information Engineering, Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China), Jiayuan Li (Institute of Information Engineering, Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China), Haiqiang Fei (Institute of Information Engineering, Chinese Academy of Sciences, China), Lun Li (Institute of Information Engineering, Chinese Academy of Sciences, China), and Hongsong Zhu (Institute of Information Engineering, Chinese Academy of Sciences, China)</i>	
FMTD: Federated Learning-Based Multi-Angle Feature Fusion Framework for Abnormal Transaction Detection in Digital Currency .....	2418
<i>Yaru Lv (Qingdao University of Science and Technology, China), Lijun Sun (Qingdao University of Science and Technology, China), and Xiao Chen (University of Leicester, UK)</i>	
Privacy Preservation in Cloud-Based Distributed Learning through Data Encoding and Partitioning .....	2424
<i>Łukasz Krzywiecki (Wroclaw University of Science and Technology, Poland), Krzysztof Szymaniak (Wroclaw University of Science and Technology, Poland), and Marcin Zawada (Wroclaw University of Science and Technology, Poland)</i>	
Backdoor Attacks Optimized through Genetic Algorithm-Driven Data Augmentation Combinations in Deep Neural Networks .....	2430
<i>Yilun Lyu (Qufu Normal University, China), Xu Ma (Qufu Normal University, China), and Yuan Ma (Qufu Normal University, China)</i>	
A Defensive Framework Against Adversarial Attacks on Machine Learning-Based Network Intrusion Detection Systems .....	2436
<i>Benyamin Tafreshian (Boston University, USA) and Shengzhi Zhang (Boston University, USA)</i>	



## TrustCom-52: Security and Privacy

Design and Implementation of Data Encryption Mechanism in Fiber Channel Network .....	2442
<i>Hongke Zhang (Xidian University, China) and Zheng Yan (Xidian University, China)</i>	
A Reliable Edge Server Deployment Algorithm Based on Spectral Clustering and a Deep Q-Network Strategy Using Multi-Objective Optimization .....	2447
<i>Zhou Zhou (Changsha University, China), Taotao Yu (Zhejiang University of Technology, China), Mohammad Shojafar (University of Surrey, UK), Xia Ou (Zhejiang University of Technology, China), and Hongbing Cheng (Zhejiang University of Technology, China)</i>	

## The International Workshop on Security, Privacy, and Trust in Artificial Intelligence (SPTAI 2024)

Shield-U: Safeguarding Traffic Sign Recognition against Perturbation Attacks .....	2453
<i>Shengmin Xu (Fujian Normal University, China), Jianfei Sun (Singapore Management University, Singapore), Hangcheng Cao (City University of Hong Kong, China), Yulan Gao (KTH Royal Institute of Technology, Sweden), Ziyang He (Zhengzhou University, China), and Cong Wu (Nanyang Technological University, Singapore)</i>	
Deepfakes: A New Kind of Adversarial Attacks against Face Recognition Systems? .....	2462
<i>Raphael Antonius Frick (Fraunhofer SIT — ATHENE Center, Germany) and Lukas Graner (Fraunhofer SIT — ATHENE Center, Germany)</i>	
AttDet: Attitude Angles-Based UAV GNSS Spoofing Detection .....	2468
<i>Luyao Wang (National Key Laboratory of Strength and Structural Integrity, Aircraft Strength Research Institute of China, China), Xiaomin Wei (Xidian University, China), Hongtao Zhang (National Key Laboratory of Strength and Structural Integrity, Aircraft Strength Research Institute of China, China), and Lingtao Jia (National Key Laboratory of Strength and Structural Integrity, Aircraft Strength Research Institute of China, China)</i>	

## The 9th International Workshop on Privacy, Data Assurance, Security Solutions for Internet of Things (PASS4IoT 2024)

IoT Vulnerability Detection using Featureless LLM CyBert Model .....	2474
<i>Sarah Binhulayyil (Cardiff University, UK; King Saud University, KSA), Shancang Li (Cardiff University, UK), and Neetesh Saxena (Cardiff University, UK)</i>	
AI Empowered Sensitive Information Detection and Anonymisation in PDF Files .....	2481
<i>Zheng Gao (University of Electronic Science and Technology of China, China) and Hongping Li (University of Electronic Science and Technology of China, China)</i>	

## TrustCom-53: Data Security and Privacy

### The International Workshop on Data Security and Privacy (Data S&P 2024)

Analysis of Data Export Business Processes Based on Petri Nets .....	2486
<i>Yongqiang Chen (Yanshan University, China), Meiqi Liu (Yanshan University, China), Jingfeng Rong (Hainan University, China), Xujie Liu (Hainan Company Limited, China Mobile Communications Group, China), Anmin Fu (Nanjing University of Science and Technology, China), Anshun Zhou (Nanjing University of Posts and Telecommunications, China; China Union(Hainan) Innovation Research Institute, China United Network Communication Group Co., Ltd, China), and Yuqing Zhang (Hainan University, China; University of Chinese Academy of Sciences, China)</i>	
Research on Lifecycle-Driven Government Data Security Model and Data Grouping Technology .	2492
<i>Siyu Chen (Hainan University, China), Jingfeng Rong (Hainan University, China), Zhiyuan Fu (Hainan University, China), Qiuling Yue (Hainan University, China), Anmin Fu (Nanjing University of Science and Technology, China), Xujie Liu (China Mobile Communications Group, China), Anshun Zhou (Nanjing University of Posts and Telecommunications, China; United Network Communication Group Co., Ltd, China), and Yuqing Zhang (Hainan University, China; University of Chinese Academy of Sciences, China)</i>	
A Review of Data Security Research in Energy Storage Systems .....	2498
<i>Meiqi Liu (Yanshan University, China), Yongqiang Chen (Yanshan University, China), Chaoyang Zhu (China Electric Power Research Institute, China), Shuang Yao (China Electric Power Research Institute, China), Jingfeng Rong (Hainan University, China), Xiaolong Zhao (Hainan University, China), Xijuan Si (University of Chinese Academy of Sciences, China), Guang Yang (Beijing HyperStrong Technology Co., Ltd, China), and Yuqing Zhang (Hainan University, China; University of Chinese Academy of Sciences, China)</i>	
Risk Assessment Based on Dataflow Dynamic Hypergraph for Cross-Border Data Transfer .....	2504
<i>Zhou Fang (Beijing University of Posts and Telecommunications, China), Kai Zhang (Beijing University of Posts and Telecommunications, China), Yigang Diao (Cyberspace Administration of China, China), Yixuan Song (Beijing University of Posts and Telecommunications, China), Yanwei Sun (Beijing University of Posts and Telecommunications, China), and Jinqiao Shi (Beijing University of Posts and Telecommunications, China)</i>	
LogContrast: Log-Based Anomaly Detection Using BERT and Contrastive Learning .....	2510
<i>Wei Yuan (Xidian University, China), Hongyu Sun (Hainan University, China), Mo Pang (Security Research Institute, China Academy of Information and Communications Technology, China), He Wang (Xidian University, China), Gaofer Wu (Xidian University, China), and Yuqing Zhang (Xidian University, China; University of Chinese Academy of Sciences, China)</i>	

A Study of Backdoor Attacks on Data Distillation for Text Classification Tasks .....	2517
<i>Sixian Sun (Yanshan University, China), Hongyu Sun (Hainan University, China), Haoxing Zhang (Security Research Institute China, Academy of Information and Communications Technology, China), and Yuqing Zhang (Yanshan University, China; University of Chinese Academy of Sciences, China)</i>	

## **TrustCom-54: Trustworthy Crowd Computing**

### **The International Workshop on Trustworthy Crowd Computing and Systems (TCCS 2024)**

Distributed Data Possession - Blockchain Based Scalability .....	2523
<i>Bartłomiej Dzikowski (Wrocław University of Science and Technology, Poland), Łukasz Krzywiecki (Wrocław University of Science and Technology, Poland), Ksawery Możdżyński (Wrocław University of Science and Technology, Poland), Karol Niczyj (Karol Niczyj Software House, Poland), and Hannes Salin (Swedish Transport Administration, Sweden)</i>	
Trusted and Spectrum-Efficient Crowd Computing in Massive MIMO Cellular Networks .....	2529
<i>Pengfeng Zhang (State Grid Shandong Electric Power Company Zibo Power Supply Company, China), Lei Li (State Grid Shandong Electric Power Company, China), Xin Liu (State Grid Shandong Electric Power Research Institute, China; Shandong Key Laboratory of Energy Industry Internet Big Data Technology, China), Rui Wang (State Grid Shandong Electric Power Research Institute, China; Shandong Smart Grid Technology Innovation Center, China), Donglan Liu (State Grid Shandong Electric Power Research Institute, China; Shandong Key Laboratory of Energy Industry Internet Big Data Technology, China), Bing Su (State Grid Shandong Electric Power Research Institute, China; Shandong Smart Grid Technology Innovation Center, China), Yuntao Wang (Xi'an Jiaotong University, China), Yiliang Liu (Xi'an Jiaotong University, China), and Zhou Su (Xi'an Jiaotong University, China)</i>	
Trustworthy Approaches to RSA: Efficient Exploitation Strategies Based on Common Modulus ...	2535
<i>Mahdi Mahdavi (Shahid Beheshti University, Iran), Navid Abapour (University of Surrey, UK), and Zahra Ahmadian (Shahid Beheshti University, Iran)</i>	
Trust Evaluation in Mobile Crowd Sensing Networks Based on Age of Trust (AoT) .....	2541
<i>Xiayue Wang (Beijing Jiaotong University, China), Mingyang Li (Beijing Jiaotong University, China), Yuting Tao (Beijing Jiaotong University, China), Xuanzhe Wang (Beijing Jiaotong University, China), and Hao Wu (Beijing Jiaotong University, China)</i>	
MT-Index: A Trustworthy Index for Multimodal Data Sharing .....	2547
<i>Qianyue Fan (Northwestern Polytechnical University, China), Shiqian Wang (State Grid Henan Electric Power Company, Economic and Technological Research Institute, China), Zhe Feng (Northwestern Polytechnical University, China), and Li Di (State Grid Henan Electric Power Company, China)</i>	

Honeybee-RS: Enhancing Trust through Lightweight Result Validation in Mobile Crowd Computing .....	2553
<i>Sanjay Segu Nagesh (Deakin University, Australia), Niroshinie Fernando (Deakin University, Australia), Seng W. Loke (Deakin University, Australia), Azadeh Ghari Neiat (The University of Queensland, Australia), and Pubudu N. Pathirana (Deakin University, Australia)</i>	

## The 18th IEEE International Conference on Big Data Science and Engineering (BigDataSE 2024)

Payload Level Anomaly Network Traffic Detection via Semi-Supervised Contrastive Learning ....	2559
<i>Xinglin Lian (Xidian University, China), Yang Liu (Xidian University, China), Shanfeng Wang (Xidian University, China), and Yu Zheng (Xidian University, China)</i>	
DualConvNet: Enhancing CNN Inference Efficiency Through Compressed Convolutions and Reparameterization .....	2567
<i>Haipeng Du (Xi'an Jiaotong University, China), Muyan Jiao (Xi'an Jiaotong University, China), Jiageng Zhang (Xi'an Jiaotong University, China), Xin Lv (Xi'an Jiaotong University, China), and Jie Zhang (Xi'an University of Technology, China)</i>	
Navigating Time's Possibilities: Plausible Counterfactual Explanations for Multivariate Time-Series Forecast through Genetic Algorithms .....	2575
<i>Gianluca Zuin (Universidade Federal de Minas Gerais, Brazil) and Adriano Veloso (Universidade Federal de Minas Gerais, Brazil)</i>	
An Experimental Study on Half-Closed TCP Connections in Public Cloud Gateways .....	2583
<i>Zhuang Yuan (Xi'an Jiaotong University, China; Tencent Inc., China), Rui Li (Xi'an Jiaotong University, China), Fa Zhang (Xi'an Jiaotong University, China), Kejing Xu (Xi'an Jiaotong University, China), Liang Xu (Xi'an Jiaotong University, China), and Weizhan Zhang (Xi'an Jiaotong University, China)</i>	
A Multi-Stage Spike Stream Processing and Image Reconstruction Method for Industrial Applications .....	2590
<i>Shuaipeng Wu (Southern University of Science and Technology; Shenzhen Institute of Advanced Technology, Chinese Academy of Sciences, China), Changhao Yuan (Shenzhen Institute of Advanced Technology, Chinese Academy of Sciences; University of Chinese Academy of Sciences, China), and Kejiang Ye (Shenzhen Institute of Advanced Technology, Chinese Academy of Sciences, China)</i>	
Fraud Detection in Supply Chain Order Management via Kolmogorov-Arnold Networks .....	2598
<i>Haowei Huo (State Grid Shaanxi Procurement Company, China), Ting Lv (State Grid Shaanxi Procurement Company, China), Ningbo Zhao (State Grid Shaanxi Procurement Company, China), Gefan Ai (State Grid Shaanxi Procurement Company, China), Qi He (Xidian University, China), Ying Kong (State Grid Shaanxi Procurement Company, China), Yu Zhang (State Grid Shaanxi Procurement Company, China), Yiwei Li (State Grid Shaanxi Procurement Company, China), Jiangyao Wei (State Grid Shaanxi Procurement Company, China), Chen Liu (State Grid Shaanxi Procurement Company, China), Yuan Liu (Xidian University, China), and Lichuan Ma (Xidian University, China)</i>	

## The 27th IEEE International Conference on Computational Science and Engineering (CSE 2024)

Multi-Scale Fuzzy Graph Convolutional Network for Hyperspectral Image Classification .....	2606
<i>Mingxin Jin (Northwestern Polytechnical University, China), Cong Wang (Northwestern Polytechnical University, China), Shanglin Yang (Peking University, China), Heng Wang (Northwestern Polytechnical University, China), Ju Huang (Northwestern Polytechnical University, China), and Jun Zhao (Nanyang Technological University, China)</i>	
RTM-CMD: Exploring Advanced Underground Target Detection in Coal Mines through Modified RTMDet Methodology .....	2612
<i>Longlong Gao (Xi'an Polytechnic University, China), Tao Xue (Xi'an Polytechnic University, China), and Long Xi (Xi'an Polytechnic University, China)</i>	
Your Data is Leaking! An Empirical Study of User Habits during Smartphone Charging .....	2619
<i>Steven Krudsen (Copenhagen Business School, Denmark) and Wenjuan Li (The Education University of Hong Kong, Hong Kong SAR; Guangzhou University, China)</i>	
Anticipated Failure Determination-Based Weakness Analysis with Common Weakness Enumeration .....	2627
<i>Toru Sakon (Notre Dame Seishin University, Japan)</i>	
Hardware Latency-Aware Differential Architecture Search: Search for Latency-Friendly Architectures on Different Hardware .....	2635
<i>Jiaqi Han (Xidian University, China), Dan Wang (Xidian University, China), Hong Luo (China Mobile (Hangzhou) Information Technology Co., Ltd, China), Ye Zhou (Xidian University, China), and Bin Song (Xidian University, China)</i>	
Large-Scale Thermo-Hydraulic Analysis of Fuel Rod Bundles Based on YH-ACT .....	2644
<i>Min Song (National University of Defense Technology, China), Chao Li (National University of Defense Technology, China), Xiaowei Guo (National University of Defense Technology, China), Jie Liu (National University of Defense Technology, China), Huajian Zhang (National University of Defense Technology, China), and Rui Xia (National University of Defense Technology, China)</i>	

## The 22nd IEEE International Conference on Embedded and Ubiquitous Computing (EUC 2024)

Machine Learning Enhanced Indoor Positioning with RIS-Aided Channel Configuration and Analysis .....	2653
<i>Yanhong Xu (Xidian University, China), Zhao Li (Xidian University, China), Ziru Zhao (Xidian University, China), Blaise Herroine Aguenoukoun (Xidian University, China), Jia Liu (Xidian University, China), Zhixian Chang (Xi'an University of Posts and Telecommunications, China), and Yicheng Liu (Xidian University, China)</i>	

An Automated PM2.5 Analysis and Prediction System with Encoder-Decoder Architecture and Continual Learning Mechanism .....	2661
<i>Le Anh Duc Vu (Hanoi - Amsterdam High school for the Gifted, Vietnam), Minh Hai Vu (Hanoi University of Science and Technology, Vietnam), Bao Ngoc Tran (Hanoi University of Science and Technology, Vietnam), Minh Tung Hoang (Hanoi - Amsterdam High school for the Gifted, Vietnam), Duc Anh Nguyen (Hanoi - Amsterdam High school for the Gifted, Vietnam), Minh Quan Hoang (Hanoi - Amsterdam High school for the Gifted, Vietnam), and Phi Le Nguyen (Hanoi University of Science and Technology, Vietnam)</i>	
Multi-Sensor Fusion-Based Cow Health Monitoring IoT System .....	2669
<i>Zhenyu Lai (Xi'an Jiaotong-Liverpool University, China), Yijia Xu (Xi'an Jiaotong-Liverpool University, China), Jialei Zhang (Xi'an Jiaotong-Liverpool University, China), Bowen Jia (Xi'an Jiaotong-Liverpool University, China), Liangyan Wang (Shenfu Dairy Farm Company, China), Qinglei Bu (Xi'an Jiaotong-Liverpool University, China), Jie Sun (Xi'an Jiaotong-Liverpool University, China), and Quan Zhang (Xi'an Jiaotong-Liverpool University, China)</i>	
A Digital Traditional Chinese Medicine Splint for Treatment of Distal Radius Fracture .....	2675
<i>Siyuan Wang (Xi'an Jiaotong-Liverpool University, China), Shuchen Liu (Xi'an Jiaotong-Liverpool University, China), Zheng Jin (Xi'an Jiaotong-Liverpool University, China), Zheng Yan (Suzhou TCM Hospital Affiliated to Nanjing University of Chinese Medicine, China), Tao Chen (Suzhou TCM Hospital Affiliated to Nanjing University of Chinese Medicine, China), Qinglei Bu (Xi'an Jiaotong-Liverpool University, China), Zhiqiang Wang (Suzhou TCM Hospital Affiliated to Nanjing University of Chinese Medicine, China), Jintao Liu (Suzhou TCM Hospital Affiliated to Nanjing University of Chinese Medicine, China), and Jie Sun (Xi'an Jiaotong-Liverpool University, China)</i>	

## **The 12th IEEE International Conference on Smart City and Informatization (iSCI 2024)**

Deep Reinforcement Learning for Active RIS-Assisted Full-Duplex Integrated Sensing and Communication Systems .....	2680
<i>Bingxin Zhang (Nanjing University, China; Nanjing University (Suzhou Campus), China), Kang Zheng (China Mobile Zijin Innovation Institute Co., Ltd., China), Chao Tong (China Mobile Zijin Innovation Institute Co., Ltd., China), Kun Yang (Nanjing University, China; Nanjing University (Suzhou Campus), China), and Kang Yan (University of Electronic Science and Technology of China, China)</i>	
A Corrected Method for Parameters in the Signal Propagation Model .....	2686
<i>Yan Liang (Chengdu Technological University, China), Xin Dong (Chengdu Technological University, China), Song Chen (Chengdu Technological University, China), Zhengda Li (Chengdu Technological University, China), and Zhimin Chang (HAN Networks Corporation Limited, China)</i>	
Research on Energy Management Strategy of Microgrid Based on Improved Deep Q Network Algorithm .....	2694
<i>Le Tian (Foshan University, China), Changshen Ou (Foshan University, China), and Weilin Huang (Foshan University, China)</i>	

A Cross-Domain Authentication Scheme Based on Quantized Trust Relationship for Smart Grid .	2701
<i>Tianang Chen (Southeast University, China), Haojie Qin (Southeast University, China), Jin Qian (State Grid Zhejiang Electric Power Company, China), Jun Luo (State Grid Zhejiang Electric Power Company, China), Yinghua Jiang (Southeast University, China), and Liquan Chen (Southeast University, China)</i>	
Long-Term Privacy-Preserving Incentive Scheme Design for Federated Learning .....	2709
<i>Xin Liu (State Grid Shandong Electric Power Research Institute, China), Rui Wang (State Grid Shandong Electric Power Research Institute, China), Pengfeng Zhang (State Grid Shandong Electric Power Company, China), Liang Xie (Xi'an Jiaotong University, China), Yiliang Liu (Xi'an Jiaotong University, China), Zhou Su (Xi'an Jiaotong University, China), Donglan Liu (State Grid Shandong Electric Power Research Institute, China), and Yingxian Chang (State Grid Shandong Electric Power Company, China)</i>	
Research on Distributed Machine Learning Defence Strategies Under Byzantine Attacks .....	2715
<i>Chen Jin (Southwest Minzu University, China), Xi Chen (Southwest Minzu University, China), Junyu Pu (Southwest Minzu University, China), and Boyu Fan (Southwest Minzu University, China)</i>	

## Author Index