

2025 IEEE 24th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom 2025)

**Guiyang, China
14-17 November 2025**

Pages 1–671

IEEE Catalog Number:
ISBN:

CFP25TRU-POD
979-8-3315-6533-6



Copyright © 2025, IEEE

All Rights Reserved

Copyright and Reprint Permissions:

Abstracting is permitted with credit to the source. Libraries are permitted to photocopy beyond the limit of U.S. copyright law for private use of patrons those articles in this volume that carry a code at the bottom of the first page, provided the per-copy fee indicated in the code is paid through Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923.

For other copying, reprint or republication permission, write to IEEE Copyrights Manager, IEEE Service Center, 445 Hoes Lane, Piscataway, NJ 08854. All rights reserved.

*** This is a print representation of what appears in the IEEE Digital Library. Some format issues inherent in the e-media version may also appear in this print version.

IEEE Catalog Number:	CFP25TRU-POD
ISBN (Print-On-Demand):	979-8-3315-6533-6
ISBN (Online):	979-8-3315-6532-9
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
Web:	www.proceedings.com

TABLE OF CONTENTS

Active-Trust Based Security Service Orchestration Framework for 6G Enabled Massive IoT	1
<i>Mingfeng Huang, Ronghui Cao, Xiaoyong Tang, Tan Deng</i>	
MSG-ImDiffusion: Multi-Scale Spatio-Temporal Diffusion Modeling for Anomaly Detection in Microservice Systems	9
<i>Ruoyao Zhang, Yuchun Guo, Yishuai Chen, Zhong Cao</i>	
UAV Assisted Multi-Attack Detection Method for Vehicular Ad Hoc Networks	17
<i>Junhui Zhang, Na Fan, Liping Ye, Jianghui Hu, Yexiong Shang, Yu Shi</i>	
Identity-Based Asymmetric Group Message Franking	25
<i>Hang Liu, Yang Ming, Aotian Cai, Chenhao Wang, Yi Zhao</i>	
Revisiting the Byzantine Resilience of Federated Reinforcement Learning: A Distillation Perspective	33
<i>Wenzheng Jiang, Ji Wang, Zhengyi Zhong, Jiangzhou Liao, Xiaomin Zhu, Flint Xiaofeng Fan</i>	
Local Midpoint Guided Topology Control Method for Elimination of Vulnerable Node in UAV Ad-Hoc Networks	42
<i>Peng Zhang, Peng Yi, Tong Duan, Zhen Zhang, Jiaxin Li, Junfei Li, Jing Yu</i>	
Backdoor-Free Node Injection Attacks Against Graph Neural Networks	54
<i>Jiasheng Qiu, Lieqing Lin, Qi Zhong, Zhenyu Liang</i>	
RaceTEE: Enabling Interoperability of Confidential Smart Contracts	62
<i>Keyu Zhang, Andrew Martin</i>	
RASKEE: A TEE-Assisted Secure Range Spatial Keyword Query in a Multi-user Setting	74
<i>Zhen Lv, Yaorong Tan, Hongwei Huo, Yanguo Peng, Youliang Tian</i>	
Dual Gradient Evaluation-Based Defense Method Against Poisoning Attacks in Federated Learning	86
<i>Zhuangzhuang Zhang, Xinhai Yan, Libing Wu, Bingyi Liu, Enshu Wang, Jianping Wang</i>	
Chaos of Functionalities: Understanding Security Risks in Heterogeneity of IoT Matter Controllers	95
<i>Yiwei Fang, Haoqiang Wang, Ze Jin, Qixu Liu</i>	
Flatness-Aware Attack: Enhancing Adversarial Transferability via Local Region Stability	103
<i>Kejun Zhang, Yufan Yang, Jiahao Cheng, Meijiao Li</i>	
TF-Detector: Anomaly Detection in Industrial Control System through Process-Aware Time-Frequency Domain Analysis	111
<i>Shuyuan Chang, Qixiao Lin, Jian Mao, Mengshuo Yuan, Yan Huo</i>	
Detection and Mitigation of Unknown Threats in IPv6 Networks via Layered Data Adaptation	119
<i>Youjun Huang, Xiang Li, Jia Zhang, Haixin Duan</i>	
Opening a Can of Worms: A Comprehensive View into the Android Debug Bridge Malware	131
<i>Huancheng Hu, Christian Doerr</i>	
Zero-Knowledge Quantized Weighted Majority Algorithm	143
<i>Li Quan, Xikun Jiang, Boris Döder</i>	

VarAgent: LLM-Enhanced Variable Name Recovery in Binaries via Reinforcement Learning and Semantic Fusion	152
<i>Yuyao Huang, Hui Shu, Fei Kang, Cong Li</i>	
AutoPentester: An LLM Agent-based Framework for Automated Pentesting	163
<i>Yasod Ginige, Akila Niroshan, Sajal Jain, Suranga Seneviratne</i>	
End-to-End Security Policy Automation with Multi-LLM Agents in Cloud-Native Systems	175
<i>Xuefei Chen, Yuqi Zhang, Haohao Liu, Xiaotong Wang, Chen Li, Bibo Tu</i>	
Hamster: Private Transformer Inference via Fully Homomorphic Encryption	184
<i>Huizhuo Wang, Zhiyong Zhang, Lei Ju</i>	
When Voices Deceive: Evaluating and Improving the Robustness of Audio Deepfake Detectors Under Adversarial Attacks	192
<i>Karla Schäfer, Leon Ludwig</i>	
Towards Automated and Robust Forensic Event Reconstruction	200
<i>Lukas Schmidt, Sebastian Schinzel</i>	
GTCN-G: A Residual Graph-Temporal Fusion Network for Imbalanced Intrusion Detection	211
<i>Tianxiang Xu, Zhichao Wen, Xinyu Zhao, Qi Hu, Yan Li, Chang Liu</i>	
Bias as an Exploit: A Scalable Red-Team Campaign to Uncover Gender-Based Vulnerabilities in Foundational Models	219
<i>Kun Jia, Jiyun Chen, Haizhen Gao, Yuxin Zhang, Qiushi Dong, Daixi Zhang, Huimei Chen, Jiayin Qi</i>	
CTIGEN: Generating Cyber Threat Intelligence Oriented Summaries Through Summarization Fine-Tuning with Domain-specific NER	227
<i>Xuhao Wan, Xiang Lin, Jianhua Li</i>	
Buffer is All You Need: Defending Federated Learning against Backdoor Attacks under Non-iids via Buffering	236
<i>Xingyu Lyu, Ning Wang, Yang Xiao, Shixiong Li, Tao Li, Danjue Chen, Yimin Chen</i>	
Leveraging large language models for SQL behavior-based database intrusion detection	244
<i>Meital Shlezinger, Shay Akirav, Lei Zhou, Liang Guo, Avi Kessel, Guoliang Li</i>	
BDT-RVOC: Block Data Truncation for Verifiable and Private Multi-Cloud Computation	255
<i>Ze Yang, Youliang Tian, Ruixin Song, Kun Niu, Mengqian Li, Jinbo Xiong</i>	
TrustMFA: A Privacy-Preserving Multi-Factor Authentication Scheme with Anonymous Credential	263
<i>Wenjun Zhu, Jianan Hong, Shiyao Wang, Kunling Li, Kun He</i>	
HARS:A Dynamic Scheduling Algorithm for Redundant Executors Based on Weighted Hypergraph Heterogeneity	272
<i>Yifan Wang, Xinjian Zhao, ZeSheng Xi, June Li, Xu Zhong, Yu Li</i>	
Targeted and Transferable Adversarial Attacks on Large Vision-Language Models via Two-Stage Region-Specific Perturbations	282
<i>Zhuoran Wang, Jiawei Zhao, Liang Zhang, Zheng Wang, Yining Hu</i>	
Blind Points Between ASR and Intent Inferring: Vulnerability Discovering via Fuzzing in-Vehicle Voice Assistance	290
<i>Peilin Luo, Wei Teng, Jiachun Li, Yan Meng, Haojin Zhu</i>	

AutoPentestAL: An automated penetration testing framework with active learning capabilities	298
<i>Xianyi Fu, Bin Liu, Cheng Zhu, Dianqiu Ma</i>	
Blind Video Watermarking Resisting Camcorder Recording Based on Spatio-temporal Synchronization	310
<i>Ming Liu, Yifeng Shu, Lansheng Han, Xianjun Gu</i>	
MEB: A Backdoor Detection Framework for Pre-training Based Malicious Traffic Detection	321
<i>Kai Wang, Jieying Zhou, Libo Yang, Weixun Li, Ziguang Jie, Zheyu Jiang, Zhiliang Wang</i>	
On the Limitations of Fuzzy Hashing for Malware Similarity: An Analysis of Vulnerable Code Detection in Malware	332
<i>Nathan Ross, Oluwafemi Olukoya, Jesús Martínez Del Rincón</i>	
Enhancing Federated Learning under Partial Participation via Proportional Variance Reduction	344
<i>Xiang Wang, Lei Tian, Chen Yang, Feilong Lin, Minglu Li</i>	
Provenance graph-based advanced persistent threats detection via self-supervised contrastive learning	352
<i>XuTao Xiang, Yanqing Yang, Yurong Qian, Kai Zhao, Linlin Zhang</i>	
EdgeTrace: A Context-Aware Anomalous Edge Detection Framework for APT Traceback	360
<i>Nianqi Yang, Zhijian Zhao, Bing Chen</i>	
T2F2L: Towards Trustworthy Fairness in Federated Learning Through A Verifiable Approach	369
<i>Ghazaleh Keshavarzkalhori, Cristina Pérez-Solà, Guillermo Navarro-Arribas, Jordi Herrera-Joancomartí</i>	
Towards Privacy-Preserving Range Queries with Secure Learned Spatial Index over Encrypted Data	377
<i>Zuan Wang, Juntao Lu, Jiazhuang Wu, Youliang Tian, Wei Song, Qiuxian Li, Duo Zhang</i>	
Scalable Distance-aware Fuzzy Private Set Intersection	389
<i>Zhenyu Xiong, Kai Chen, Xingwei Ren, Yongqiang Li, Mingsheng Wang</i>	
The Sound of Reduction: Minimal Inputs, Maximal Coverage	401
<i>Iaroslav Gridin, Antonis Michalas, Alejandro Cabrera Aldaya</i>	
SPPF: A Speech-Semantic and Privacy-Preserving Framework with Prompt-Tuning Large Language Models	410
<i>Ben Niu, Tiantian Kong, Yuqiao Hou, Bohao Li, Guoli Zhao</i>	
Antenna Selection and Artificial Noise-based Security Transmission for Large-Scale MIMO Systems	418
<i>Shiguo Wang, Jie Ma</i>	
FlexiGrain: A Flexible and Fine-Grained Privacy Control Framework for Dynamic Social Networks	425
<i>Ben Niu, Fanyu Gan, Jinyu Peng, Qian Yang, Jin Cao</i>	
Multi-Directional Dynamical Framework for Information Propagation Prediction	433
<i>Yuhang Wang, Ziang Hu, Guangxi Wang, Yu Shang, Jizhong Han, Tao Guo</i>	
Toward Robust Encrypted Traffic Detection via Graph Contrastive Learning	441
<i>Jiahao Huang, Mohan Li, Yanbin Sun, Yu Jiang</i>	
APT-GCM: Advanced Persistent Threats Detection via Graph Contrastive Masked Representation Learning	449
<i>Mengkun Zhao, Jing Liu, Wenqiang Hao, Xiaobing Pei</i>	
BreachHydra: Measuring the Resilience of an Underground Data Breach Forum	461
<i>Marius Brockhoff, Lukas Schmidt, Fabian Ising, Sebastian Schinzel</i>	

Mixture of Experts Representation Learning Scheme for Multi-View Android Malware Detection	472
<i>Jiaxiong Chen, Shuaishuai Tan, Jinchuan Liu, Zehua Zhang, Jianjun Zhou, Qiannan Lin, Haowen Tan</i>	
Trust-Aware V2V Charging Coordination via Hierarchical Decision under Mode Uncertainty	484
<i>Shuohan Liu, Wei Zhang, Yue Cao, Qiang Ni, Lu Zhang, Xinyu Li</i>	
SCodeGen: A Real-Time Trustworthy Constrained Decoding Framework for Secure Code Generation with LLMs	492
<i>Muzi Qu, Jie Liu, Liangyi Kang, Shuyi Ling, Shuai Wang, Dan Ye, Tao Huang</i>	
Efficient Auditing and Querying in Verifiable Redactable Blockchain: A Lightweight VDS Protocol with Integrity Verification	504
<i>Xiaoxu Zhang, Zhipeng Cai, Keyan Chen, Guanxiong Ha, Chunfu Jia</i>	
Theoretical Min-Entropy Bounds for Physical-Layer Key Generation over Weibull Fading Channels	512
<i>Dongchi Han, Yuan Ma, Xianhui Lu</i>	
LLM-Driven APT Analysis and Detection Based on Provenance Graph by Threat Pattern	524
<i>Yibin Fu, Zhaoyun Ding, Sheng Zhang, Deqi Cao, Yi Wang</i>	
LDP: Latent Diffusion-based Adversarial Purification towards Transformer-based Visual Encoders	532
<i>Mengfan Li, Xinxin Fan, Quanliang Jing, Shaoye Luo, Yunfeng Lu, Jingping Bi</i>	
Non-Restrictive Hardware-Based Trust in Embedded High-Level Operating Systems	540
<i>Simon Unger, Sven Gebauer, Stefan Katzenbeisser</i>	
Compacting Side-Channel Measurements With Peak-Anchor-Based Alignment	548
<i>Yuling Luo, Minjiao Pei, Shunsheng Zhang, Xue Ouyang, Qiang Fu, Sheng Qin, Junxiu Liu</i>	
Proactive Radio Frequency Fingerprinting-Based Authentication Leverage IQ Perturbation	556
<i>Siqi Pei, Shiyue Huang, Hongbo Liu, Haitao Jia, Yanzhi Ren, Huan Dai, Jiadi Yu</i>	
Reliable and Robust Watermarking for Data Flooding against Ransomware Random Techniques	566
<i>Saverio Giallorenzo, Simone Melloni, Pietro Sami</i>	
Finder6: Efficient IPv6 Addresses Scanning Based on Hostname Correlation in IPv6-Only Network	578
<i>Ce Sun, Liancheng Zhang, Ruijuan Wang, Yakai Fang, Hongtao Zhang, Haojie Zhu, Luyang Li</i>	
RecZTA: A Reputation-Based Architecture with Dual-Layer PEPs for Zero Trust Access	586
<i>Zhi Lin, Lin Yan, Zan Zhou, Yongfeng Yu, Penghui Xiao, Shujie Yang</i>	
TCP-Awareness Augmented Robust TLS Traffic Classification: A Hybrid Deep Learning Approach	594
<i>Yewa Li, Yitan Huang, Bo Jiang, Zhigang Lu, Zelin Cui</i>	
OUF: Oblivious Universal Function with domain specific optimizations	602
<i>Victor Delfour, Marc-Olivier Killijian</i>	
Secure Communication Protocols and Video Streaming Demonstrations in Open RAN through DTLS and LKH	610
<i>Sudarson Karmaker, Haitham Cruickshank, Mohammad Shojafar</i>	
Defending Federated Learning against Backdoor Attacks by Inspecting Sparsity-Guided Out-of-Distribution Model Behavior	618
<i>Songgao Tu</i>	

Privacy-Preserving Facial Authentication with Hybrid Fuzzy Commitment and Cancelable Transformation	626
<i>Weilai Guo, Shuaichao Song, Yeming Yang, Yuming Liao, Jiyan Li, Songhui Guo</i>	
Assessing the Effectiveness of Singling-Out Attacks on Synthetic Data: Is the Current GDPR Guidance Adequate?	636
<i>Fatima Jahan Sarmin, Atiquer Rahman Sarkar, Noman Mohammed</i>	
Enhancing Physical Security in Smart Environments with Ambient Intelligence	644
<i>Ashish Nanda, Robin Doss, Folmer Heikamp, Abhi Kumar, Haftu Reda, Adnan Anwar, Zubair Baig Praveen Gauravaram, Debi Prasad Pati, Salil Kanhere, Mohan Baruwal Chhetri</i>	
CVshield: Interpretable Black-Box Adversarial Defense for LLMs via CoT Guided Semantic Verification	656
<i>Wenjing Hu, Weiwei Qi, Yanlu Li, Xinzhe Huang</i>	
An Efficient Feature Extraction Model Based on Asymmetric Deep Convolutional Autoencoder for Abnormal Traffic Detection	664
<i>Guofeng Zhang, Yang Zhang, Bingbing Wang</i>	
KSFed: A Defense against Poisoning Attacks in Federated Learning using Statistical Analysis	672
<i>Jiaxuan Zhao, Qi Feng, Qin Liu, Min Luo, Wei Zhao, Debiao He</i>	
MalShield: Enhancing Android Malware Detection with Stateful Defense against Query Attacks	681
<i>Hengyu Zhang, Guang Cheng, Yuyang Zhou, Zongyao Chen</i>	
MBCGAN-SGFM: Detecting Rare and Unknown Attacks via Generative Augmentation and Semantic Memory	690
<i>Yunhao Wang, Yong Wang, Lin Zhou</i>	
Can We Distinguish? A Deep Learning Approach to AI-Generated Content Detection	700
<i>Yikai Liang, Mengqing Liu</i>	
RuDyna: Towards A Dynamic Analysis Framework for Rust	708
<i>Shanlin Deng, Baojian Hua</i>	
DCIAD: Dual CNN with Informer for Time-Series Anomaly Detection	720
<i>Xiang Zhong, Yong Wang, Lin Zhou</i>	
Solving Small LWE Instances with the Dropping Meet-in-the-Middle Algorithm	730
<i>Xiaofei Tong, Jingguo Bi, Shuwen Luo, Licheng Wang, Lixiang Li, Lin Wang</i>	
ET-FS: Functional Specialization Method for Multi-Task Learning in Encrypted Traffic Classification	738
<i>Xinzhu Feng, Gaopeng Gou, Chang Liu, Zheyuan Gu, Wenqi Dong, Famei He, Xuren Wang</i>	
APER: An Efficient and Privacy-Preserving Scheme for E-Health Recommendations	750
<i>Jing Wang, Wenhao Yuan, Xianjun Deng, Qiankun Zhang, Jing Fan, Xue Yuan</i>	
A Trust-Based Data Quality Assessment Mechanism in Crowdsensing Services	761
<i>Hai Liu, YaDong Peng</i>	
Rusty: Effectively Detecting Multilingual Rust Memory Bugs with Interprocedural Static Analysis	769
<i>Mingliang Liu, Baojian Hua</i>	

OptiFLIDS: Optimized Federated Learning for Energy-Efficient Intrusion Detection in IoT	781
<i>Saida Elouardi, Mohammed Jouhari, Anas Motii</i>	
Attribute-Based Conditional PRE: A Novel Construction from LWE for Cloud Data-Sharing	793
<i>Lisha Yao, Jian Weng, Pengfei Wu, Guofeng Tang, Haiyang Xue, Guomin Yang, Robert H. Deng</i>	
A secure and provable deletion method over outsourced data for fog-based smart grid	805
<i>Changsong Yang, Yueling Liu, Yong Ding, Hai Liang, Shuo Wang</i>	
MLSBOX: Automated Sandbox for Fine-Grained Isolation of Multiple Third-Party Libraries*	813
<i>Yuqi Qiu, Juan Wang, Chenjun Ma, Yunfeng Kang, Jie Wang</i>	
RL-Optimized Lightweight Obfuscation Against Binary Code Similarity Detection	825
<i>Ran Wei, Hui Shu, Fei Kang</i>	
Building Provably Secure Pseudo-Strong PUFs via Weak PUFs and Pseudorandom Functions for Cryptographic Protocols	837
<i>Chenghao Chen, Xiaolin Zhang, Kailun Qin, Tengfei Wang, Yipeng Shi, Tianyi Huang, Chi Zhang Dawu Gu</i>	
Controller Makes Pentesting Better: An Improved Multi-Agent Automated Penetration Testing Framework	845
<i>Xiaoyu Geng, Ning An, Boyuan Xu, Xiaobo Yang, Bo Jiang, Baoxu Liu, Junrong Liu</i>	
Bits for Privacy: Evaluating Post-Training Quantization via Membership Inference	853
<i>Chenxiang Zhang, Tongxi Qu, Zhong Li, Tian Zhang, Jun Pang, Sjouke Mauw</i>	
AlignAD-VAE: A Variational Autoencoder with MMD-Based Dataset Alignment for Network Anomaly Detection	861
<i>Samed Saka, Valerio Selis, Alan Marshall</i>	
PANDA-CDR: Perturbation-Aware and Neural Dual-Channel Alignment for Cross-Domain Recommendation	868
<i>Ruohan Wang, Gaode Chen, Miaobo Hu, Ji Xiang, Ruixin Song, Cong Xue, Lei Wang, Haoyuan Teng</i>	
Decentralizing Photo Forensics for Public and Verifiable Trust	878
<i>Mauro Clavijo-Herrera, Rolando Trujillo-Rasua, Carles Anglés-Tafalla</i>	
ConCloneDep: A Confidence-Aware Clone-Based Dependency Identification Approach in C/C++ Open-Source Components	886
<i>Jianxing He, Xi Chen, Shan Yao, Xiaoyan Liang, Ruizhong Du</i>	
ComplexMM: Efficient and Generic Homomorphic Matrix Multiplication via Complexification and BSGS Alignment	894
<i>Yucen Liao, Junping Wan, Jingjing Fan, Zoe L. Jiang</i>	
EFSM-Based Modeling of Siemens S7comm for Adaptive Cyber Deception in ICS Honeypots	903
<i>Saurabh Chamotra, Ferdous Ahmed Barbhuiya</i>	
Securing AI Code Generation - A Prompt Rectification Approach for Mitigating Cyber Risks	914
<i>Jialiang Dong, Zihan Ni, Nan Sun, Sanjay Jha, Yiwei Zhang, Elisa Bertino, Surya Nepal, Siqi Ma</i>	
Mitigating Leakage Amplification in DP-Enhanced Encrypted Search Across Multiple Users	926
<i>Yingying Qi, Jiabei Wang, Tiancheng Zhu, Yongbin Zhou</i>	

Prototype-Integrated Representation Learning for Novelty Detection	934
<i>Saranya Vijayakumar, Christos Faloutsos, Matt Fredrikson</i>	
Robustness Assessment and Enhancement of Text Watermarking for Google's SynthID	942
<i>Xia Han, Qi Li, Jianbing Ni, Mohammad Zulkernine</i>	
Clean Label Backdoor Attack Based on Feature Distance Guided Sample Selection and Noise Optimization	950
<i>Lixia Xie, Pengcheng Kang, Hongyu Yang, Juncheng Hu</i>	
Data Driven Based Attention Mechanism for Optimal Anomaly Detection in Complex Multivariate Time Series Data	958
<i>Shubha Dhali, Kuntal Ghosh, Siddhartha Prakash Duttagupta</i>	
On-Chain Risk Signals: Predicting Security Threats in DeFi Projects	966
<i>Bahareh Parhizkari, Antonio Ken Iannillo, Ed Zulkoski, Christof Ferreira Torres, Radu State</i>	
PROV-LLM: Advanced Persistent Threat Detection Based on Process Behavior Subgraphs Using Large Language Models	978
<i>Canhua Chen, Yang Song, Yunpeng Li, Yun Feng, Xiaoyu Wang, Yuling Liu, Qixu Liu</i>	
Reinforcement Learning Enhanced Temporal Generative Adversarial Networks for Blockchain Illicit Transaction Detection	986
<i>Mengyuan Li, Jiewei Chen, Shaoyong Guo, Xue-Song Qiu, Feng Qi</i>	
A Zero-Trust Empowered Continuous Authentication System for Drivers: Integrating Federated Learning with Conditional Transformer GAN	996
<i>Lina Ge, Zhipeng Cao, Ming Jiang, Liang Zhao</i>	
ReTainer: Reputation-Aware Containerized Service Deployment in Blockchain Networks	1007
<i>Xiaoxu Ren, Qixin Li, Haipeng Yao, Tianhao Ouyang, Ruichen Zhang</i>	
Trusted Online Key Management Center Architecture and Implementation Method for Train Control Systems	1015
<i>Weihong Ma, Xinxin Li, Xiaoya Hu, Shaohu Li, Qian Wang, Fangyu Li</i>	
Artificial Noise-Based Countermeasure Against Full-Duplex (FD) Active Eavesdropping	1023
<i>Shiguo Wang, Yun Zhao</i>	
From Text to STIX: Reducing Hallucinations through Fine-Tuned LLMs	1030
<i>Ruoyao Xiao, Yu Luo, Weifeng Xu, Dianxiang Xu</i>	
Adversarial Example Based Fingerprint Embedding for Robust Copyright Protection in Split Learning	1038
<i>Zhangting Lin, Mingfu Xue, Wenmao Liu, Liquan Chen</i>	
Scalable Private k-Nearest Neighbors Search Based on Secret Sharing	1046
<i>Peizhao Zhou, Lihai Nie, Zheli Liu</i>	
PrivRAG: A Privacy-Preserving Retrieval-Augmented Generation Protocol for LLM-Driven Voice Assistants	1054
<i>Yuan Chang, Siran Wang, Tom H. Luan, Yuntao Wang, Zhou Su</i>	
Interprocedural Call Graph Embedding with GAT for Memory safety Vulnerability Detection	1062
<i>Rong Ren, JingYi Wu, HongBo Jin, QingYu Song, Bing Zhang, Qian Wang</i>	

PUF-Enhanced Physical-Layer Key Generation for Secure Drone Communication with Untrusted Relays	1072
<i>Tao Chen, Dongming Li, Xianglin Fan, Yi Lou</i>	
Enhancing Adversarial Robustness of IoT Intrusion Detection via SHAP-Based Attribution Fingerprinting	1080
<i>Dilli Prasad Sharma, Liang Xue, Xiaowei Sun, Xiaodong Lin, Pulei Xiong</i>	
Deep Learning Assisted Reverse Engineering: Recognizing Encryption Loops in Ransomware	1092
<i>Nanqing Luo, Haizhou Wang, Zhilong Wang, Lan Zhang, Ping Chen, Peng Liu</i>	
KHAD: K-Hop and Activation-aware Defense against Bit-Flip Attacks in Deep Neural Networks	1103
<i>Jiajun Guo, Hao Ying, Zhezhaoyang, Xinyue Yu, Tianqi Shi, Jie Xiao</i>	
Flow-Based Screen-Shooting Robust Watermarking with Invertible Noise Simulation Network	1111
<i>Pei Gan, Xuehu Yan, Hu Deng, Rongtao Liao, Feng Chen</i>	
You May Not Be Your Username: Cross-Market Vendor Alias Attribution with Automatic Multi-Signal Evaluation	1119
<i>Wesley H. Kwan, Lynn K. Takahashi, Nathan Pham, Apurva Sista, Ericsson Marin</i>	
Establishing Secure Intra-Solid Communication Networks via Acoustic Transceivers	1127
<i>Chaoyi Sun, Henglin Pu, Junyi Zhou, Chao Cai</i>	
ForgeDAN: An Evolutionary Framework for Jailbreaking Aligned Large Language Models	1135
<i>Siyang Cheng, Gaotian Liu, Rui Mei, Yilin Wang, Kejia Zhang, Kaishuo Wei, Yuqi Yu, Weiping Wen Xiaojie Wu, Junhua Liu</i>	
Overcoming Data Mining in Blockchain-Based Covert Communication: Transaction Withdrawal and Multisig Embedding	1147
<i>Jialing He, Zhuo Chen, Yijing Lin, Jiacheng Wang, Liehuang Zhu, Zhu Han, Rahim Tafazolli, Tao Xiang</i>	
Dynamic Hybrid Backdoor Attack: Saliency-Guided Composite Triggers for Image Classification	1158
<i>Yuanhao Shen, Ying Wang, Yiran Liu, Zili Yao, Qiu Xue-Song, Shaoyong Guo</i>	
Machine Learning-Based Detection of AI-Generated Text via Stylistic and Statistical Feature Modeling	1166
<i>Karla Schäfer, Martin Steinebach</i>	
FedRand: A Federated Random Forest Learning Technique for Anomaly Detection in IoT Networks	1174
<i>Omodolapo Babalola, José Cano, Somrudee Deepaisarn, Nguyen Truong</i>	
TLISA: Transfer Learning Enhanced Link Stealing Attacks on Graph Neural Networks	1182
<i>Zhenkun Jin, Jiaqi Ma, Yuanyuan He, Wei Xiang, Qiankun Zhang, Tao Zhang</i>	
AMD: Adaptive Adversarial Training Method Based on Mahalanobis Distance	1190
<i>Aoqi Ruan, Hui Xia, Rui Zhang, Xiaoxue Song, Zhengheng Li, Mengyuan Song</i>	
Who Appraises the Appraiser? Decentralized Attestation with Partial Appraisal and Aggregated Results	1198
<i>Michael Eckel, Georgios Gkoktsis, Markus Horn</i>	
Hardware-Aware Neural Architecture Search for Real-Time Automotive Intrusion Detection	1210
<i>Xuke Yan, Linxi Zhang</i>	
PrivANN: Practical and Efficient Private Approximate Nearest Neighbor Search	1218
<i>Xuan Chen, Shujie Cui, Joseph K. Liu, Shi-Feng Sun, Shangqi Lai</i>	

Efficient and Privacy-Preserving (α , β)-Core Community Search over Encrypted Bipartite Graphs	1227
<i>Xiaoxian Liu, Chen Chen, Xueqiao Liu, Xiaoyang Wang</i>	
Hyperchaos and HVS-Adaptive Video Watermarking Embedding	1235
<i>Kesong Wu, Maowei Li, Peng Yang, Wanting Yang, Jiangtian Nie, Xianbin Cao</i>	
Range Dynamic Searchable Symmetric Encryption: Combating Volume Leakage and Enabling Non-interactive Deletion	1243
<i>Jinguo Li, Qiang Lv, Junqin Huang, Linghe Kong</i>	
Multidimensional Dynamic Trust Evaluation towards Intelligent Transportation	1252
<i>Kaixuan Luo, Chuanxiang Ma</i>	
Identification of Generative Forged Western Blot Images	1260
<i>Yunqiao Zhang, Shunquan Tan, Jiwu Huang</i>	
NFDP: Enabling Noise-Adaptive and Fast-Converging Privacy Protection in Graph Neural Network Training	1268
<i>Hang Chen, Bo Yin, Binyao Xu</i>	
An Adaptive Fast Recovery Scheme Based on Checkpoints: Analysis and Application in Asymmetric Multiprocessor Systems	1275
<i>Jingjing Hu, Yu Li, Yuanhang Sun, Chidan Zhu, Qinrang Liu, Jiangxing Wu</i>	
Privacy-Preserving Average Consensus by One-Step Perturbation	1283
<i>Hanyu Zhao, Yinyan Zhang</i>	
A Blockchain-Enabled AIoT Framework for Secure Metaverse in Wireless Communication Networks	1291
<i>Danhuai Zhao, Chen Tian, Zhenyu Ju, Yi Rong, Xiaoming He, Wanting Yang</i>	
Privacy-Preserving Distributed Optimal Consensus of High-Order Nonlinear Multi-Agent Systems	1298
<i>Yuxuan Xiong, Yinyan Zhang</i>	
FABA: Breaking Defenses in Production-Grade Federated Learning for Mobile Malware Detection Services	1307
<i>Xingyu Lu, Yang Cao</i>	
PDD-FANs: Personalized Decentralized Federated Adversarial Networks with Defense Mechanism in Non-IID Setting	1317
<i>Xinguang Wang, Nguyen Linh Trung, Oliver Y. Chen, Jeroen Van Schependom, Stijn Denissen, Guy Nagels</i>	
PLAA: Packet-level Adversarial Attacks in Network Traffic Detection	1327
<i>Jinhao You, Zan Zhou, Shujie Yang, Yi Sun, Lei Zhang, Changqiao Xu</i>	
Adaptive Temperature-Enhanced Hypergraph Contrastive Learning with Reliable Data Sampling Augmentation	1337
<i>Junzheng Li, Hongtao Yu, Ruiyang Huang, Suchang Yang</i>	
SEMA: A Structural Entropy Guided Multimodal Framework for Adversarial Face Attacks	1343
<i>Ruixin Song, Youliang Tian, Mengqian Li, Ze Yang</i>	
Location Privacy Protection for Network-RTK VRS Positioning Users via Mobile Networks	1351
<i>Ruoting Xiong, Yi Ren, Xin Shi, Wei Ren, Gerard Parr</i>	

A Robust and Efficient Authentication Protocol for Intelligent Systems in Smart Healthcare IoMT	1357
<i>Zaid Ameen Abduljabbar, Vincent Omollo Nyangaresi, Mustafa A. Al Sibahee, Junchao Ma</i>	
<i>Zaid Alaa Hussien, Ali Hasan Ali, Husam A. Neamah, Ahmed Ali Ahmed</i>	
Pure Object Detection for Text-CAPTCHAs – YOVO: A Lightweight Recognition Model and Annotation Framework Derived from YOLOv8n	1365
<i>Disen Tang</i>	
FDLLM: A Dedicated Detector for Black-Box LLMs Fingerprinting	1374
<i>Zhiyuan Fu, Junfan Chen, Lan Zhang, Ting Yang, Jun Niu, Hongyu Sun, Ruidong Li, Peng Liu, Jice Wang</i>	
<i>Fannv He, Yuqing Zhang</i>	
Safety-Aware DRL Training Based on Reachability Analysis	1380
<i>Yixuan Yang, Min Zhang</i>	
ETCFF: An Encrypted Traffic Classification Method Based on Fusion Features	1388
<i>ZhiPeng Fu, FanPing Zeng</i>	
Privacy-Assured Analytics on Decentralized Graphs:The Case of Graph Learning	1396
<i>Longji Li, Yifeng Zheng, Songlei Wang, Zhongyun Hua, Lei Xu, Yansong Gao</i>	
FTE: Filter-Based Trust Evaluation for the Internet of Vehicles	1406
<i>Hai Lin, Xingchen Zhu, Zhihong Chen, Yue Cao</i>	
Efficient and Dynamic Multi-Source Data Analytics over Encrypted Cloud Data with Bitmap-Based Indexing	1416
<i>Yuyang Wang, Wei Song, Ruisi Song, Yuan Shen, Xiaohui Wang</i>	
PPFDroid: An Android Malware Detection Method Based on Pre-Training and Prompt-Based Fine-Tuning	1425
<i>Xufeng Wang, Yuqi Ma, Hongxian Liu, Sanfeng Zhang</i>	
CyberSOIE-LLM: Cybersecurity Semi-Open Information Extraction with Large Language Models	1435
<i>Xinzheng Liu, Zhaoyun Ding</i>	
A Class of Semi-Supervised Weighted Nonnegative Matrix Factorization for Community Detection	1443
<i>Shibo Jin, Shiqi Liu, Lujuan Dang</i>	
TriDNet: 3D Reconstruction and Generalized Feature Disentanglement for Deepfake Detection	1451
<i>Yaqi Liu, Hanhan Wang, Weichen Zhu, Kunbai Zhang, Chao Xia</i>	
SafeMLLM: Extending Safety Alignment from Single-Modal LLMs to Multimodal LLMs	1457
<i>Di Jiang, Xiaojie Zhu, Chi Chen</i>	
BayesFuzz: Bayesian-Based Greybox Fuzzing for Stateful Protocols	1466
<i>Jianwen Xiang, Junwei Jiang, Songsong Liao, Xueming Zhang, Rui Hao</i>	
Attention-Inverse Perturbation: A Novel Adversarial Attack Strategy by Targeting Non-Attentive Regions	1472
<i>Ming Zhang, Zhendong Wu, Hu Li, Jin Li, Ling Pang, Cheng Qian</i>	
TSDAs: Enhanced Statistics-Based Query Recovery in Dynamic Searchable Symmetric Encryption via Probabilistic Modeling	1479
<i>Yikang Fan, Xiaojie Zhu, Chi Chen, Yong Li</i>	

POLARIS: Cross-Domain Access Control via Verifiable Identity and Policy-Based Authorization	1489
<i>Aiyao Zhang, Xiaodong Lee, Zhixian Zhuang, Jiuqi Wei, Yufan Fu, Botao Peng</i>	
Granular Ball and Curriculum Learning-Based Fuzzy Support Vector Machine	1499
<i>Zhenlei Wu, Xiaoqin Pan, Lei Zhou</i>	
Exploring the Relationship Between Network Similarity and Transferability of Adversarial Attacks	1507
<i>Gerrit Klause, Niklas Bunzel</i>	
Model Evaluation-Driven Aggregation: FedMEDA for Robust Non-IID Federated Learning	1513
<i>Bosong Zhang, Linna Zhang, Qian Sun, Hai Wang, Danyang Li</i>	
Post-Quantum Cryptography for Secure Authentication Key Distribution in QKD Networks	1522
<i>Filip Lauterbach, Lukáš Kapičák, Sergej Jakovlev, Miralem Mehic, Stefan Rass, Miroslav Voznak</i>	
Fine-Grained Revocable Lattice-Based ABE: Dual User and Attribute Revocation with Low Overhead for Cloud Environments	1533
<i>Yuliang Liu, Yuan Liu, Yiwen Gao, Yongbin Zhou, Licheng Wang, Peng Gao</i>	
TrustMonitor: A Secured Container Framework via Virtualization and Pointer Authentication for Cross-Domain Data Sharing	1541
<i>Xin Wang, Yulun Song, Fan Zhang, Feng Qi, Yunlong Xie, Lin Sun</i>	
Disguised Attack in the Metaverse: A New Threat to Avatar-Based Identity Security	1553
<i>Chen Zhang, Zhenyong Zhang, Cong Wang, Ruilong Deng</i>	
Retrieval-Augmented Generation-Based Adaptive State Enhancement for Federated Split Learning	1561
<i>Boyang Dong, Xiukun Yan, Kai Zeng</i>	
Efficient and Secure Spatial Keyword Similarity Query with User Preference	1569
<i>Shen Du, Xinrui Ge, Chengliang Tian</i>	
TrapLLM: An LLM-powered Interactive Log-based Honeypot for Real-world Network Attacks	1578
<i>Yunjun Ma, Gangyan Zeng, Peng Zhang, Yuchen Huang, Fuyuan Zhang, Ran Lin, Huan Qian</i>	
An Efficient FHE-based Ciphertext Matrix Multiplication Algorithm	1586
<i>Yihan Wang, Xiangjun Xue, Jingyong Liang, Donghai Guan, Çetin Kaya Koç</i>	
Cross-Modal Collaborative Recovery: Breaking Multimodal Unlearnable Examples Protection	1592
<i>Ruijia Li, Zijiao Zhang, Ximin Huang, Hongwei Hu, Xining Gao</i>	
A Systematic Approach to Predict the Impact of Cybersecurity Vulnerabilities Using LLMs	1598
<i>Anders Mølmen Høst, Pierre Lison, Leon Moonen</i>	
VLAH: A Lightweight and Verifiable Framework for Approximate Nearest Neighbor Search in High-Dimensional Space	1608
<i>Yiping Teng, Yuyao Tang, Gang Wang, Shiqing Wang, Changze Li, Liang Zhao</i>	
Leveraging Cross-Layer Network Probing to Detect Stealth Services	1617
<i>Jiangyi Yin, Chenxu Wang, Zhao Li, Zhuojun Jiang, Jiangchao Chen, Dongfang Hao, Qingyun Liu</i>	
Post-Quantum Anonymity of Key Encapsulation Mechanism and Its Applications in Password Authenticated Key Exchange Protocols	1626
<i>JiaYv An, Yankun Gao, Lei Han</i>	

An Improved Vector Commitment Construction with Applications to Signatures	1634
<i>Yalan Wang, Bryan Kumara, Harsh Kasyap, Liqun Chen, Sumanta Sarkar, Christopher J.P. Newton</i> <i>Carsten Maple, Ugur Ilker Atmaca</i>	
User Demands Based Multi-Agent Reinforcement Learning Satellite Handover Strategy*	1640
<i>Qiyun Yu, Yanrong Lu, Weiwei Jiang</i>	
Privacy-preserving Location-Based Services with A New Private Information Retrieval Scheme	1649
<i>Xiaopang Wang, Lihui Wang, Limin Guo</i>	
No Touch, No Trace: A Paradigm for Remote Voltage Side-Channel Attacks on FPGA-Based Computing Platforms	1661
<i>Zhe Liu, Kun Zhou, Chengkai Chen, Jianfei Mao, Hongbing Cheng</i>	
Automated Attack Graph Construction for Cross-host Threat Detection Using Cyber Threat Intelligence	1671
<i>Chen Ling, Yifei Li, Ziqing Feng, Bin Liu, Qiuyun Wang, Liling Xin, Zhengwei Jiang, Huamin Feng</i>	
Accelerating Privacy-Preserving Federated Learning in Large-Scale LEO Satellite Systems	1679
<i>Binquan Guo, Junteng Cao, Marie Siew, Binbin Chen, Tony Q. S. Quek, Zhu Han</i>	
Toxic Ink on Immutable Paper: Content Moderation for Ethereum Input Data Messages (IDMs)	1687
<i>Xihan Xiong, Zhipeng Wang, Qin Wang, William Knottenbelt</i>	
SoK: Credential-Based Trust Management in Decentralized Ledger Systems	1697
<i>Yanna Jiang, Haiyu Deng, Qin Wang, Guangsheng Yu, Xu Wang, Yilin Sai, Shiping Chen, Wei Ni</i> <i>Ren Ping Liu</i>	
SERA: Semantic Entity Recognition and Alignment for Threat Intelligence Representation	1707
<i>Xinyu Liu, Tianbo Wang, Chunhe Xia, Yingming Zeng, Ruidong Wang</i>	
TGF-JA4: LLM-Aware Multi-Feature Temporal Graph For Malware Detection Under Concept Drift	1716
<i>Xinyan Chen, Yu Wang, Peishuai Sun, He Wang, Yuqing Zhang</i>	
CrossMiner: Smart Contract Vulnerability Detection in Interactive Scenarios	1724
<i>Xiangfu Liu, Teng Huang, Caiyan Tan, Jiahui Huang, Qiong Wang, Yan Pang</i>	
Adaptive Neuron Honeypot: Trapping Malicious Backdoors in Federated Learning	1733
<i>Xingyu Lu, Yang Cao</i>	
Optimizing FHE-Based Secure Matrix Computation for Untrusted Cloud Environments	1742
<i>Yuanyuan Xie, Ming Luo, Han Wang, Mingsheng Wang</i>	
CoDA: Cross-Domain Few-Shot Website Fingerprinting via Contrastive Prototype Alignment	1752
<i>Yongxin Li, Yuwei Xu, Xinhe Fan, Yujie Hou, Yali Yuan, Qiao Xiang, Guang Cheng</i>	
A Privacy-Preserving and Highly Fault-Tolerant Cross-Chain Atomic Swap Scheme	1759
<i>Wenjun Zhu, Jianan Hong, Yingjie Xue, Jiayue Zhou, Shiyao Wang</i>	
Exploring Subtle Manipulation Vulnerabilities in Federated Distillation	1765
<i>Peiyan Chen, Changsheng Wan, Hao Zou, Tian Wen, Zhiyuan Wu</i>	
PACT: A Passive Accuracy-Based Trust Metric for Malicious Client Detection in Federated Learning	1775
<i>Sayedali Sheykhoslamzadeh, Dima Alhadidi</i>	
LASEFlow: A Label-Aware Security Enhancement Framework for Serverless Workflows	1782
<i>Minghui Chen, Keming Wang, Chenlin Huang, Fengyuan Yu, Renyu Yang, Hua Cheng, Mantun Chen</i>	

A Dual-Stage Anomaly Detection Framework for Stealthy Attacks in 5G Core Networks	1791
<i>Xin Feng, Cong Li, Weizhi Meng, Zilong Wang, Xinsheng Ji</i>	
Detecting Content Rating Violations in Android Applications: A Vision-Language Approach	1799
<i>Dishanika Denipitiyage, Bhanuka Silva, Suranga Seneviratne, Aruna Seneviratne, Sanjay Chawla</i>	
A Comprehensive Analysis of the AKMA+ Protocol	1809
<i>Yueming Li, Long Chen, Zhenfeng Zhang</i>	
From Sample Generation to Efficacy Transfer: Optimization of Privacy-Preserving LLMs for Content Moderation	1819
<i>Mingyong Yin, Tong Liu, Hejun Wang, Yulong Wang, Run Yang</i>	
MR-Patch: A Retrieval-Augmented Generation Approach for Patch Presence Test	1829
<i>Zirui Jiang, Yisen Wang, Xingyu Bai, Jiajun Du, Tianchan Yang, Bing Zhu</i>	
SwCC: A Swapped-Contrastive Clustering Learning for Few-shot Website Fingerprinting Attacks	1839
<i>Jing Bai, Gaopeng Gou, Zheyuan Gu, Wenqi Dong, Gang Xiong, Zhen Li, Zhenzhen Li, Qingya Yang</i>	
FedPPA: Progressive Parameter Alignment for Personalized Federated Learning	1849
<i>Maulidi Adi Prasetya, Muhamad Risqi U. Saputra, Guntur Dharma Putra</i>	
Beyond Algorithmic Proofs: Towards Implementation-Level Provable Security	1857
<i>Jiahui Shang, Luning Zhang, Zhongxiang Zheng</i>	
DFAFuzz: Fuzzing for Embedded JavaScript Virtual Machines with Type-Directed DFA	1867
<i>Haiwei Lai, Baojian Hua</i>	
Security Risks of Transpiling C Programs to Rust	1877
<i>Si Wu, Huyao Yang, Baojian Hua</i>	
DoNotSurf - Low-Latency DNS IP Tunneling	1887
<i>Alexandru Kiraly, Darius Vasile Bufnea</i>	
VCR: Fast Private Set Intersection with Improved VOLE and CRT-Batching	1895
<i>Weizhan Jing, Xiaojun Chen, Xudong Chen, Ye Dong, Yaxi Yang, Qiang Liu</i>	
MVL-AD: A Multi-View Learning Framework for Class-Incremental Unknown Attack Detection	1905
<i>Xukui Li, Guang Cheng, Wei Chen, Zhen Zhang, Zechen Xu, Xing Qiu</i>	
Traceable and Revocable Key-Policy Attribute-Based Encryption scheme from Lattices	1914
<i>Yanqi Ma, Yuan Liu, Yongbin Zhou, Yiwen Gao</i>	
Secure Non-Interactive Authentication in Satellite Networks Using Time Lock Encryption	1921
<i>Xinhong Hei, Xi Zuo, Yichuan Wang, Mengjie Tian, YanHua Feng</i>	
Intrusion Detection via Federated Learning: Tackling Non-IID Data and Poisoning Attacks	1929
<i>Quan Li, Yuhong Li</i>	
PathFed: Trustworthy and Efficient Federated Aggregation via Path Attention	1936
<i>Manzhou Li, Xinjin Ge, Yan Li, Yan Zhang</i>	
High-fidelity Dual-layer Backdoor Watermarking Scheme based on Private Model Embedding	1944
<i>Lingyun Xiang, Fangbo Luo, Xiangli Jin</i>	

Security of LLM Agents: A Case Study Approach	1952
<i>Casey Fan, Diyana Tial, Vladislav Dubrovenski, Mengtao Zhang, Yugyung Lee, Dianxiang Xu</i>	
LENI: Lightweight and Efficient Network-Optimized Remote Attestation for IoT Devices	1958
<i>Michael Eckel</i>	
STAR-Shield: Self-Tuning Adaptive Rules for Web Application Firewall-as-a-Service via Multiple Large Language Models	1968
<i>Letian Sha, Lei Xue, Nan Yi, Fu Xiao</i>	
Recipient-Agnostic Hash Locks for Cross-Chain Auctions with Bitcoin Bidding	1976
<i>Fuyang Deng, Qianhong Wu, Bo Qin</i>	
Broken Chains: An Empirical Analysis of DNS Resolution in IPv6-only Environments	1985
<i>Lei Zhao, Yujia Zhu, Baiyang Li, Yong Sun, Yuedong Zhang, Qingyun Liu</i>	
A Threshold Distributed Key Generation and Dynamic Key Management Scheme in Wireless Sensor Networks	1993
<i>Wenhui Kong, Pengfei Wen, Bo Li, Heng Gao, Runshan Hu, Ning Hu, Xingjun Wang</i>	
PoDIBC: Prevention of DrDoS Attacks Using Identity -Based Cryptography in Software-Defined Networking Environment	2002
<i>Shain Saharan, Vishal Gupta</i>	
Hierarchical Ring Signatures with Hidden Signature Functionality over Blockchain Infrastructure	2010
<i>Łukasz Krzywiecki, Witold Karaś, Adam Niezgoda, Karol Niczyj</i>	
Multi-Party Contract Signing Ensuring Trust in Complex Transactions	2016
<i>Cătălin V. Bîrjoveanu, Mirela Bîrjoveanu</i>	
FakeZero: Real-Time, Privacy-Preserving Misinformation Detection for Facebook and X	2025
<i>Soufiane Essahli, Ouassama Sarsar, Imane Fouad, Ahmed Bentajer, Anas Motii</i>	
From static to dynamic risk indicators in predicting and detecting insider attacks	2036
<i>N'Famoussa Kounon Nanamou, Rim Ben Salem, Anis Bkakra, Nora Cuppens-Boulahia, Frédéric Cuppens</i>	
Verifiable and Robust Distributed Deep Learning based on Blockchain Infrastructure	2044
<i>Mikołaj Pietrek, Łukasz Krzywiecki, Karol Niczyj, Witold Karaś</i>	
Zephyr: Secure and Non-interactive Two-Party Inference for Transformers	2050
<i>Wenchao Liu, Huiyu Xie, Tanping Zhou, Shuo Chen, Weidong Zhong, Xiaoyuan Yang</i>	
Fairness-Constrained Optimization Attack in Federated Learning	2060
<i>Harsh Kasyap, Minghong Fang, Zhuqing Liu, Carsten Maple, Somanath Tripathy</i>	
TwinGuard: A Proactive RL-Driven Defence Framework for Digital Twin-Enabled O-RAN Security	2066
<i>Neha Gupta, Liam O'Driscoll, Taneya Sharma, Mohammad Shojafar, Chuan Heng Foh, Ioana Boureanu Helen Treharne, Sotiris Moschoyiannis</i>	
Leader-Follower Federated Learning Framework: Heterogeneous Federated Learning based on Asymmetric Distillation	2072
<i>Lina Ge, Haisong Zhu, Ming Jiang, Zhe Wang</i>	
LLM-Assisted IDOR Detection in Hospital Mini-Programs: Risks to PII and PHI	2078
<i>Jiawen Sun, Rui Tian, Shangru Zhao, Xiangming Zhou, He Wang, Yuqing Zhang</i>	

AuthVR: Securing Authentication Against Shoulder Surfing and Keystroke Inference Attacks using Virtual Reality	2087
<i>Md Yeasin Ali, Touhid Islam Uday, Md. Ishmam Tasin, Masum Alam Nahid, Fairuz Rahaman Chowdhury Farida Chowdhury, Md Sadek Ferdous</i>	
LDInfer: Landmarks Inference-Based for Facial Forgery Detection of Different Quality	2097
<i>Jiaxin Jiang, Zhiwen Chen, Hui Zhou, Wenjun Yan, Tianshuo Jiao, Bohan Tan, Zhuo Zhang, Hao Chen Zheng Qin</i>	
Comparing Reconstruction Attacks on Pretrained Versus Full Fine-tuned Large Language Model Embeddings on Homo Sapiens Splice Sites Genomic Data	2105
<i>Reem Al-Saidi, Erman Ayday, Ziad Kobti</i>	
GMFuzz: Integrating Hierarchical Mutation and Fidelity Constraints for Coverage-Guided DNN Security Testing	2115
<i>Yue Cui, Guangshun Li, Kexin Yang, Junhua Wu</i>	
SSRCorr: A Self-Supervised Robust Flow Representation Learning Framework for Flow Correlation Attacks on Tor	2123
<i>Chen Chen, Mengyan Liu, Zhong Guan, Yaochen Ren, Yanbo Wu, Yangyang Guan, Zhen Li, Gaopeng Gou Junzheng Shi</i>	
RegMix: Adversarial Mutual and Generalization Regularization for Enhancing DNN Robustness	2131
<i>Zhenyu Liu, Varun Ojha</i>	
Towards a Deep Understanding and Practical Guideline on the SameSite Policy	2139
<i>Shuang Wu, Ying Yu, Yan Liu, Xiangyu Gao, Zhe Qu</i>	
A New End-to-End Encrypted Image Retrieval Scheme in Cloud Environment	2149
<i>Yanfeng Chen, Jing Liang, Hongliang He, Peiya Li</i>	
Real-Time Forgery Detection via Dynamic Frequency-Domain Selection and Phoneme Alignment	2156
<i>Wenbin Li, Peng Yang, Xiaoyu Geng, Kesong Wu, Hongtao Yu</i>	
FaultSpy: On the Insecurity of SPDm Protocols under Fault Injection	2163
<i>Peiyao Sun, Qifan Wang, David Oswald, Mark Dermot Ryan, Vladimiro Sassone, Ahmad Atamli</i>	
QUICKly Running Out of Money: Evaluating QUIC Resilience to Traffic Inflating Attacks	2173
<i>Giovanni Menon, Enrico Bassetti, Mauro Conti</i>	
CatPoison: Category-Oriented Knowledge Poisoning Attacks in Retrieval-Augmented Generation Systems	2181
<i>Haitao Mei, Zhangzhuo Du, Chao Cai, Chi Cheng, Jian Chen</i>	
CyberNER: A Harmonized STIX Corpus for Cybersecurity Named Entity Recognition	2190
<i>Yasir Ech-Chammakhy, Anas Motii, Anass Rabii, Oussama Azrara, Jaafar Chbili</i>	
L2M-AID: Autonomous Cyber-Physical Defense by Fusing Semantic Reasoning of Large Language Models with Multi-Agent Reinforcement Learning	2198
<i>Tianxiang Xu, Zhichao Wen, Xinyu Zhao, Jun Wang, Yan Li, Chang Liu</i>	
DeFiAD: A Unified Method for Early-Stage Domain Abuse Detection Through Automated Deep Feature Interaction	2204
<i>Zhaojun Dai, Xiaodong Lee, Yufan Fu, Botao Peng</i>	

ORThrus: Detecting Deep Learning Compiler Bugs via Optimization Resistance Transformations	2214
<i>Tongwei Zhang, Baojian Hua</i>	
Improved Differential-Linear Distinguishes on the ChaCha256 Stream Cipher	2224
<i>Honglei Wang, Lin Ding, Zhengting Li, Xinhai Wang</i>	
A Watermarking Framework for Secure Distribution of Meteorological Images	2231
<i>Yue Wu, Fenghua Li, Feng Lu, Zifu Li, Yixuan Zhang, Yanru He</i>	
Pruning for Security: Mitigating Stealthy Bit-Flip Attacks with Efficiency Gains	2239
<i>Hao Ying, Jiajun Guo, Xinyue Yu, Zhezhaoyang, Tianqi Shi, Jie Xiao</i>	
Privacy-Preserving and Control-Compliant Authenticated Access for the AI-Enabled Industrial Internet of Things	2247
<i>Qing Fan, Yumeng Xie, Zhitao Guan, Yongshuang Wei, Yajie Wang, Chuan Zhang, Liehuang Zhu</i>	
Jailbreaking Multimodal Large Language Models via Consistent Cross-Modal Backgrounds	2259
<i>Meng Yang, Peirou Liang, Zhiqian Wu, Yong Liao</i>	
Two-Tier Batch Data Integrity Verification with Identity-Based Signatures and Privacy Preservation in Cloud-Edge-End Architecture	2267
<i>Xiuping Li, Yong Li, Yangbai Zhang, Wen Sun, Xiaowei Li, Xiaolin Chang</i>	
Incorporating Statistic and Semantic Dependencies for Enhancing the Robustness of Android Malware Detection	2273
<i>Lingyu Qiu, Zhen Liu, Bitao Peng, Ruoyu Wang, Changji Wang, Qingqing Gan</i>	
D ³ FL: Label-Free and Heterogeneity-Robust Defense for Federated Learning via Distilled Reference Model against Data Poisoning Attacks	2283
<i>Hongliang Yin, Hongjiao Li</i>	
TAR – PCH: Traceable and Revocable Blockchain Rewriting via Partial Policy-Hiding Chameleon Hashing under Cloud Assistance	2291
<i>Lifeng Guo, Jingjing Xie, Runtao Zhang, Wei-Chuen Yau</i>	
NFD-TRG: Network Flow Detection via Traffic Relationship Graphs with Statistical Feature Embedding	2301
<i>Mingshu He, XiaoWei Zhao, Liu Yang</i>	
A Transferable Adversarial Attack Framework for Object Detection via Spatial-Frequency Information Masking	2311
<i>Zhipeng Lyu, Xiumei Li, Junmei Sun</i>	
FST-AD: Anomaly Detection for Cyber-Physical Systems via Frequency-Spatio-Temporal GNNs	2319
<i>Zhenya Chen, Xueying Bian, Ming Yang, Chensheng Liu, Xiaoming Wu, Sihan Lu</i>	
Model Reduction of Colored Petri Nets Based on Unrelated Transitions	2327
<i>Zhen Gao, Tao Sun</i>	
FBFISADetector: A Method based on Filter Mechanism to detect the Instruction Set Architecture of Monolithic Firmware	2337
<i>Qing Yang, Shangru Zhao, Yuqing Zhang</i>	
A Heterogeneous GNN Based Trust Evaluation Method for Remote Desktop Access	2346
<i>Haishuo Zhang, Huiran Yang, Hongjia Li, Yan Zhang, Peng Chen, Weiping Wang, Ding Tang</i>	

Hybrid Fault Attack on Grain-128AEAD: Signature or Machine Learning Localization with Bandit-Guided Recovery	2355
<i>Ya Lin, Iftekhhar Salam</i>	
Towards System-of-Systems Bill of Material Solution for Vulnerability Operational Impact Analysis	2363
<i>Lucas Tesson, Jamal El Hachem, Patrice Guillou, J��r��my Buisson</i>	
Assessing the Impact of Post-Quantum Digital Signature Algorithms on Blockchains	2373
<i>Alison Gon��alves Schemitt, Henrique Fan da Silva, Roben Castagna Lunardi, Diego Kreutz Rodrigo Brand��o Mansilha, Avelino Francisco Zorzo</i>	
Trust-Aware Rapid Emergency Service Recovery for Low-Altitude Intelligent Networking via Transformer-Enhanced Reinforcement Learning	2381
<i>Lixin Zhang, Peng Yu, Chaochao Li, Can Tan, Xu Chen, Dingshi Liao</i>	
Adaptive Cooperative Spectrum Sharing in HSTNs with Hardware Impairments and Realistic Fading for Enhanced Reliability	2387
<i>Arshaq Saldin, Ammar Hawbani, Yunchong Guan, Yunhe Sun, Saeed Hamood Alsamhi, Liang Zhao</i>	
Improving Reliability of Electric-Vehicle Charging Service: A Scalable Modeling Approach	2393
<i>Xiuping Li, Yong Li, Yangbai Zhang, Xiaowei Li, Xiaolin Chang</i>	
Hotness Strategy based Secure Cross-user Deduplication for Cloud Storage	2399
<i>Liangyu Zhang, Junyu Cheng, Xin Tang, Jiaxin Li</i>	
DataLineage RCA: Root Cause Diagnosis for Data Lineage Issues Using Large Language Model-Based Agents	2407
<i>Xin Yi, Shangru Zhao, Yuqing Zhang</i>	
Comparative Analysis of Cross-Border Data Flow Policies: EU, US, and China	2413
<i>Zhoujie Rong, Jingfeng Rong, Yuqing Zhang</i>	
Review of Defect Detection Techniques for Power Information Systems	2419
<i>Xingwang Dou, Shanquan Yang, Chaoyang Zhu, Ziqing Lin, Baiji Hu, Jice Wang, Hongyu Sun, Fannv He Anmin Fu, Yuqing Zhang</i>	
Log Intelligent Knowledge Base Construction Method Based On Streaming Graph Fusion	2427
<i>Xinzhuo Xue, Shangru Zhao, Yuqing Zhang</i>	
OSSDetector: Towards a More Accurate Approach for C/C++ Third-Party Library Detection	2433
<i>Xiang Hai, Jia Zeng, Zhiyuan Fu, Siyu Chen, Yansong Shi, Hongyu Sun, Jice Wang, Fannv He Yuqing Zhang</i>	
Beyond Likes: Unraveling the Veil of Personal Data Exposure in Mobile Application GUIs	2439
<i>Jice Wang, Fannv He, Yue Fang, Yuqing Zhang</i>	
MAD-OOD: A Deep Learning Cluster-Driven Framework for an Out-of-Distribution Malware Detection and Classification	2445
<i>Tosin Ige, Christopher Kiekintveld, Aritrn Piplai, Asif Rahman, Olukunle Kolade, Sasidhar Kunapuli</i>	
Multi-keyword Searchable Encryption Scheme with Policy Hiding Support for User Revocation in Cloud Environment	2451
<i>Xuan Zhang, Suzhen Cao, Tianhao Zhang, Guorui Liu, Lei Han, Xiaodong Yang</i>	

iSME: Image Steganography with MECS Based on GAN	2461
<i>Yamin Li, Chen Zeng, Liu Duan, Xuansong Li, Can Li, Haofeng Ju</i>	
Diffusion-Driven Video Steganography: A Three-Stage Framework for Robust and High-Capacity Data Concealment	2471
<i>Yuning Zhou, Min Wu, Hongxiang Ji, Ziwei Wang</i>	
DAPUR: A Decentralized Anonymous Payment Under Regulation from Bitcoin	2479
<i>Yu Zhang</i>	
Evasion Attacks in Continual Learning	2486
<i>Niklas Bunzel, Aino Schwarte</i>	
Verifiable Outsourced CP-ABE with Authority Audit for Public Computing Devices	2492
<i>Dan Gao, Huanhuan Xu</i>	
SemiFlow: Website Fingerprinting Using Semi-Supervised Learning	2500
<i>Shanpeng Lv, Ying Yang, Yuling Huang</i>	
Evaluating Behavior Graph Reduction Strategies for Machine Learning-Based Malware Detection	2509
<i>Samy Bettaieb, Serena Lucca, Charles-Henry Bertrand Van Ouytsel, Etienne Rivière</i>	
A Region Dual-Factor Aware Federated Learning Framework for NWDAF in B5G/6G Core Network	2517
<i>Mingchuang Zhang, Hongbo Tang, Wei You, Xingxing Liao, Jie Yang, Hang Qiu</i>	
TeGCN: Temporal Evolution-Aware Trust Evaluation for Dynamic Social Networks	2527
<i>Chunhui Liu, Geming Xia, Chaodong Yu, Yuze Zhang, Jiawen Wu, Hongwei Huang</i>	
An Evolutionary Algorithm with Advanced Initial Solutions for Association Rules Hiding	2536
<i>Jiaran Qiu, Peng Cheng, Jun Zhou</i>	
Blockchain-Verified Attribute-Based Keyword Search with User-Generated Keys in Multi-owner Setting for IoT	2544
<i>Zongmin Wang, Qiang Wang, Fucui Zhou, Bao Li, Jian Xu, Haoyan Huang</i>	
Goal Hijacking Attack on Large Language Models via Pseudo-Conversation Injection	2552
<i>Zheng Chen, Buhui Yao</i>	
A Privacy-Preserving Aggregation Scheme Based on Dual-Masking and Threshold Signature in Computing Power Network	2558
<i>Xiaodong Yang, Junru He, Na Wang, Duoqia Wang, Yuanxin Zhang, Yatang Zhong</i>	
Profile: Self-Supervised Communication Relationship Profiling for Imbalanced Smart Grid Anomaly Detection	2566
<i>Haimiao Li, Changbo Tian, Runqing Zhang, Shiyi Yuan, Bo Sun</i>	
Bad-PoseDiff: Pose-Guided Backdoor Triggering in Diffusion Models	2574
<i>Jiahao Chen, Yu Pan, Lin Wang, Yi Du</i>	
Fair Data Exchange Scheme with Cryptographic Commitment and Smart Contract for Data Trading	2582
<i>Xiaomei Yan, Yong Li, Yan Zhu</i>	
P ³ G: A Privacy-Preserving Password Guessing Model via Cross-Task Feature Sharing	2588
<i>Wei Yu, Cheng Tan, Lvlin Ni, Chengyu Du, Cheng Liu, Qingbing Ji</i>	

SATA: A Distributed Stealthy and Persistent Backdoor Attack via Trigger Association in Federated Learning	2598
<i>Xin Ai, Yang Cao</i>	
PrivFGL: Differentially Private Federated Graph Learning via Personalized Data Transformation	2606
<i>Songyan Zhang, Hanyu Lu, Hongfa Ding</i>	
A Blockchain-Based Spectrum Allocation Scheme Based on Beneficial Consensus Mechanism	2612
<i>Peiliang Zuo, Yuexiang Wang, Zhen Fang, Xuegang Wang</i>	
Learning to Co-Design Routing and Processing in Computing Power Networks	2622
<i>Ye Qin, Kexian Liu, Jianli Liu, Xiaolong Hu, Zejun Lan, Jianfeng Guan</i>	
Ghost Vehicle: A Game-Theoretical Attack Strategy Targeting CAV Platoons	2632
<i>Lanai Huang, Winston Ellis, Sana Belguith</i>	
IAGNN: Mitigating Quantity and Topological Imbalance for Fair Graph Learning	2642
<i>Yangqi Liu, Xuemin Wang, Liang Chang, Heng Yang</i>	
GraphAss: Multi-dimensional dependency semantics graph-based Automobile software vulnerability detection method	2652
<i>Qingwen Han, Shiyu Sun, Jianmei Lei, Lingqiu Zeng, Yang Liu, Lei Ye, Kaiwei Fan</i>	
SPFuzz: Program-State-Aware Fuzzing for Mail Protocols	2660
<i>Hangzhou Fei, Xiaobing Xiong, Hui Shu</i>	
A New Key Expansion Scheme for SM4 based on Sponge Construction	2670
<i>Xin Yu, Juan Xu, Xiaoxiao Zhang, Jian Lei</i>	
Improved Rsqrt for Faster Secure Neural Networks Inference	2676
<i>Jiafu Liu, YeDong, Yuqi Zhou, Jun Huang</i>	
GPEA: Grad-CAM-Guided Perceptibility-Reduced Ensemble Attack in Object Detection	2683
<i>Zhengheng Li, Hui Xia, Rui Zhang, Mengyuan Song, Aoqi Ruan, Shaoqiang Wang</i>	
BinFuse: Binary Code Similarity Detection via Lightweight Fused Semantic Embedding	2689
<i>Shengjia Chang, Baojiang Cui, Shaocong Feng</i>	
Robust Recovery Method Against Malicious Face Swapping in Online Social Networks	2697
<i>Huaquan Yang, Shan Bian, Gongwei Weng</i>	
FedProbe: Attacking Federated Model Ownership Verification via Fine-Grained Watermark Detection and Erasure	2703
<i>Kunlong Jin, Youliang Tian, Lujia Shi</i>	
Improving the SEU Reliability of TMR Designs Implemented on SRAM-Based FPGAs with Redundant Module Restructuring	2711
<i>Chidan Zhu, Jingjing Hu, Yuanhang Sun, Yu Li</i>	
CLEK-HP: A certificate-less efficient key agreement scheme based on hybrid PUF in VANETs	2719
<i>Junfeng Tian, Tingting Jin, Ni Rui</i>	
CAHS-Attack: CLIP-Aware Heuristic Search Attack Method for Stable Diffusion	2729
<i>Shuhan Xia, Jing Dai, Hui Ouyang, Yadong Shang, Dongxiao Zhao, Peipei Li</i>	

GVTMC: A Novel Cryptocurrency Mining Traffic Classification Method	2735
<i>Yujie Lai, Huiyong Liu, Wei Zhang</i>	
PPIA-MTL: Efficient Property Proportion Inference Attacks on Tabular Generative Models via Multi-Task Learning	2743
<i>Ninghui Zhang, Chun Long, Jing Li, Fan Yang, Yuhao Fu, Wei Wan, Haojie Nie, Xingbo Pan</i>	
Ultra-Reliable Routing Strategy for Large-Scale Optical Free-Space Low Earth Orbit Satellite Networks	2753
<i>Haowen Wu, Wei Ren, Yong Wang, Yan Zhang</i>	
Hybrid Multi-granularity Reconstruction and Contrastive Learning for Graph Anomaly Detection	2759
<i>Mingjie Yu, Jiong Yu</i>	
A High-Quality Data-Driven Incentive Mechanism for Multi-Platform Mobile Crowdsensing	2766
<i>Minghe Zhang, Xuanyu Wang, Lihong Chen, Gang Liu</i>	
WSDNet: A Dual-Branch Wavelet-Structured Network for Image Forgery Detection	2774
<i>Xiao Ke, Song Yun</i>	
Passkeys in Practice: An Empirical Evaluation of FIDO2/WebAuthn Compliance and Interoperability	2781
<i>Ahmed Mahfouz, Rawad Abdulghafor, Alaa A. K. Ismaeel</i>	
A Trustworthy and Efficient Inference Scheduling Scheme for Edge MoEs Using DRL	2789
<i>Jinyang Zhang, Shengli Pan, Shanwu Chen, Anandarup Roy, Peng Li</i>	
5GC-PDA: A Novel Proactive Defense Architecture for Enhancing 5G Core Network Security	2795
<i>Xingxing Liao, Wei You, Jie Yang, Jian Tao, Runhan Feng, Xinsheng Ji</i>	
Capodoglio: Tackling Multi-Armed Bandit Jamming Attacks	2803
<i>Shuo Wang, Alessandro Brighente, Valeria Loscri, Junqing Zhang, Mauro Conti</i>	
Asteroid X: A Decentralized Finance Platform for Mining Sectors	2811
<i>Ben Chen, Xingyu Yang, Hui Cui, Joseph K. Liu</i>	
A Cross-Layer Attribution Method Based on Cyber-Physical Coupling Under Load Redistribution Attack	2818
<i>Zhenya Chen, Rongbin Yao, Chensheng Liu, Ming Yang, Xiaoming Wu, Wenting Wang</i>	
Splicing Strategy based Chunk Level Deduplication Scheme for Cloud Storage	2827
<i>Xin Tang, Haixin Chen, Siyu He, Yamin Yang, Luchao Jin</i>	
Lattice-based Dynamic Privacy-preserving Cross-chain Payment Scheme	2835
<i>Bing Zhang, Guijuan Wang, Zhongyuan Yu, Anming Dong, Hongliang Zhang</i>	
Early Classification and Improved Performance: A Multi-Model Serial Encrypted Traffic Classification Framework	2843
<i>Jinhui Li, Guang Cheng, Zihan Chen</i>	
RESA: RLWE-Based Efficient Secure Aggregation For Federated Learning	2852
<i>Ziming Wang, Liang Zhang, Hang Zhou, Haibin Kan, Jiheng Zhang</i>	
PIRL: A Robust and Privacy-Preserving Learning Method from an Information-Theoretic Perspective	2860
<i>Guangyuan Liu, Shigong Long</i>	
Log2Sig: Frequency-Aware Insider Threat Detection via Multivariate Behavioral Signal Decomposition	2868
<i>Kaichuan Kong, Dongjie Liu, Xiaobo Jin, Zhiying Li, Guanggang Geng</i>	

Multi-Channel Attacks on Dilithium: Bridging Power Gaps with EM-Guided Synthetic Traces	2877
<i>Qikang Fan, Jingdian Ming, Yiwen Gao, Yongbin Zhou</i>	
FedDHKD: A Lightweight Federated Learning Framework Based on Dynamic Hierarchical Knowledge Distillation for 5G IoT	2885
<i>Junxuan Lv, Qiwei Zhao, Hongbo Tang, Hang Qiu, Wei You, Yu Zhao</i>	
Engine-Agnostic Evaluation of Container Isolation Characteristics	2894
<i>Felix Wruck, Maximilian Peisl, Michael Weiß</i>	
Zero Trust-Based Dynamic and Continuous Access Control for Mobile Devices	2904
<i>Xiaoya Cao, Zhenya Chen, Ming Yang, Xin Wang, Xiaoming Wu</i>	
HOT-SPT: Hierarchical Optimal Transport for Robust and Fair Cross-Domain Video Expression Recognition	2911
<i>Qianli Zhao, Zhen Wang, Linlin Zong, Chao Jin, Xiaohuan Li</i>	
PSI-TR-ABE: A Traceable and Policy-Hidden Attribute-Based Encryption Scheme for Medical Data Sharing	2917
<i>Ye Feng, Siqi Lu, Liujia Cai, Xingyun Hu, Xinxin Wang, Yongjuan Wang</i>	
Efficient Zero-Knowledge Proofs for Typical Non-Linear Functions in Machine Learning	2927
<i>Shengqi Jin, Weihai Li, Zongyang Zhang</i>	
Clue Discovery based on Multi-modal Entity Alignment enhanced by Image Generation and Structure Embedding	2937
<i>Chunqing Yu, Chengxiang Tan, Zhishuo Zhang, Jiacheng Xu, Jianpeng Hu, Xiangyun Kong</i>	
DeepLancet: Effectively Detecting Deep Learning Library Bugs via LLM-assisted Testcase Generation	2944
<i>Zihao Luo, Baojian Hua</i>	
Towards Stateless Post-Quantum Remote Attestation for IoT Using TPM and DICE	2954
<i>Michael Eckel, Janik Gorbracht, Georgios Gkoktsis, Tobias Kaupat</i>	
Layered Website Fingerprinting Defense Against Adversarial Training	2966
<i>Yong Zeng, Jiaze Li, Hao Liu, Zhihong Liu, Jianfeng Ma</i>	
An Autoencoder-Based Black-Box Adversarial False Data Injection Attack Against Smart Grid	2972
<i>Juntao Zhang, Chensheng Liu, Xin Wang, Ming Yang, Xiaoming Wu</i>	
UC Secure Privacy-Preserving and Auditable Transaction System for Permissioned Blockchains*	2978
<i>Su Hang, Guo ZhaoZhong, Xu Maozhi</i>	
Diverse Fault Attacks on Dilithium and Variant Implementation: Skipping, Aborting and Zeroing	2986
<i>Hao Yuan, Yuejun Liu, Jingdian Ming, Yongbin Zhou</i>	
LLM-Guided Mutation Location Selection for Vulnerability-Aware JavaScript Engine Fuzzing	2994
<i>Jizhe Li, Yongjun Wang, Haoran Xu, Lin Peng, Muxin Xu, Tian Xia</i>	
Combining Evolutionary Learning and Window Method for Finding Short Addition Chains for Large Integers	3000
<i>Xiaopeng Zhao, Zhusen Liu, Jiawei Qian</i>	

Privacy for AI Generated Images: Conditional Generative Adversarial Networks Trained Over Obfuscated Data	3005
<i>Krzysztof Tałałaj, Łukasz Krzywiecki, Marcin Zawada</i>	
LDFS: LLMs with Dynamic Few-Shot for Offensive Language Detection	3011
<i>Yimin Wang, Qian Huang, Kaizhi Wu, Kai Guo</i>	
FedEdge: Federated Self-Supervised Graph Learning with Personalized Fine-Tuning for Node Classification	3017
<i>Zichao Deng, Han Yu</i>	
A Real-Time Defense Framework Using PPPO in Deep Reinforcement Learning for CyberBattleSim	3024
<i>Yixuan Cao, Aniket Mahanti, Ranesh Naha</i>	
VMPL-KMI: Protecting Kernel Module Integrity within Confidential VMs	3032
<i>Benshan Mei, Wenhao Wang, Dongdai Lin</i>	
Validation of a Governance Framework Supporting Security Controls across Emerging Systems	3038
<i>Maysa Sinan, Mojtaba Shahin, Iqbal Gondal</i>	
A Robust Federated Learning Framework Integrating Principal Component Analysis and Dual Detection Mechanisms	3047
<i>Lina Ge, JianWei Zhai, Qinchun Su</i>	
HyBiGraph: Toward Multi-Order Malicious Encrypted Traffic Classification via Hyper-Bipartite Graph Fusion	3053
<i>Yibin Zhou, Yunxiao Shi, Xiao Yang, Da Xiao, Gaolei Li, Jianhua Li</i>	
A Privilege Creep-Aware Role Mining Method for Enhanced Access Control Security	3063
<i>Vincent Bittard, Rim Ben Salem, Ahmed Bouzid, Sara Imene Boucetta, Frédéric Cuppens Nora Cuppens-Boulahia</i>	
Semantic-Graph-Indistinguishability: A Novel Approach to Location Privacy Protection Under Road Networks	3072
<i>Sai Wang, Huijuan Lian, Lei Shi, Gaolei Li, Yan Cao</i>	
Robust Multi-Scale Gradient Estimation for Query-Efficient Black-box Adversarial Attack	3081
<i>Guorong Wang, Jinchuan Tang, Zehua Ding, Youliang Tian</i>	
DTAHF-Net: Domain-Trust Alignment and Hierarchical Fusion for Multimodal Fake News Detection	3087
<i>Lexin Feng, Jiayin Wei, Youjun Lu, Fujian Feng</i>	
SecuRecNet-IoT: Adaptive Secure Reconfiguration and Session-Aware Communication in IoT Edge Networks	3097
<i>Osama Mohammed Dighriri, Priyadarsi Nanda, Manoranjan Mohanty, Bashair Alrashed, Ibrahim Haddadi</i>	
IEPIS: An Intelligent Endpoint Protection and Insight System	3103
<i>Rahul K. Patel, Puya Pakshad, Amandeep S. Batra, Shubhayan Das, Alapan Ghosh</i>	
Detecting Multi-Turn Jailbreak Attacks in Large Language Models via Linear Probes	3111
<i>Jorge Marina-Metola, Jose Maria de Fuentes, Lorena Gonzalez-Manzano, Luis Ibanez-Lissen</i>	
DerandomPre: An LLM-based Stability Enhancement Method for Network Protocol Fuzzing	3121
<i>Yifan Zhang, Kailong Zhu, Qian Chen, Zixiong Li, Yuliang Lu, Yingchun Chen</i>	

Proactive Federated Backdoor Unlearning via Two-Phase Optimization and State Replacement	3131
<i>Ze Chai, Yijing Lin, Zhipeng Gao, Zhiqiang Xie, Dusit Niyato</i>	
AdaptiveWatermark: Dynamic Watermarking for Large Language Models with Agent	3137
<i>Qingze Peng, Daifeng Li</i>	
Contrasting Crypto and Exfiltration Ransomware with Shamir's Secret Sharing Data Flooding	3143
<i>Daniele D'Ugo, Saverio Giallorenzo, Simone Melloni</i>	
GAPPO: Graph-Attention Enhanced Reinforcement Learning for Efficient Attack Path Planning	3152
<i>Xiuping Li, Yong Li, Yangbai Zhang, Wen Sun, Xiaowei Li, Junchao Fan, Xiaolin Chang</i>	
Fed-CMA: Federated Clustering and Matched Averaging for Personalized Intra-Vehicular Network Intrusion Detection	3158
<i>Louis Agnese, Xiaojie Lin, Guangsheng Yu, Xu Wang</i>	
TrustIoT: Building Trust in Human-Thing Interactions for Healthcare Systems Using Machine Learning	3164
<i>Abir Al-Ansari, Kristiaan D'Août, Valerio Selis</i>	
HiFi-XAI: A Fidelity-Aware, LLM-Powered Framework for Trustworthy Intrusion Detection	3171
<i>Avinash Awasthi, Pritam Vediya, Hemant Miranka, Ramesh Babu Battula, Priyadarsi Nanda</i>	
Incentive-Compatible Pricing for Truthful Data Sharing	3177
<i>Mingjian Tang, Weiqi Wang, Shui Yu</i>	
Secure Computation Scheme for the Intersection Area of Polygons Resistant to Malicious Participants	3185
<i>Xin Liu, Anyang Qi, Lanying Liang, Dan Luo, Yuchen Zhang, Wei Ye, Baohua Zhang, Yu Gu, Gang Xu Xiubo Chen</i>	
Enhancing Data Security in RISC-V Embedded Systems: A Lightweight Architecture	3195
<i>Dunkai Mao, Lifeng Xi, Fujia Zhang</i>	
Online Reliability Assessment of Nuclear Power Components via Mechanistic and Data-Driven Modeling	3201
<i>Xiangyu Jiang, Yixiong Feng, Zhiwu Li, MengChu Zhou, Xuanyu Wu, Jianrong Tan</i>	
TrustSciAgent: Towards Rigorous and Trustworthy Agents for Scientific Research	3207
<i>Yang Li, Meng Wang, Mengting Zhang, Zhixiong Zhang, Guangyin Zhang, Hanyu Li</i>	
Blockchain-Enabled Privacy-Preserving Medical Data Sharing with Verifiable Insurance Evaluation	3215
<i>Junhan Li, XiuBo Chen, Gang Xu</i>	
Human-Machine Collaborative Cognition for Intelligent Operation of Cascade Filtration Systems: A Dynamic Decision Framework Based on Fuzzy Inference and Uncertainty Analysis	3221
<i>Zhengqin Zhu, Junjie Song, Peiyan Pan, Yixiong Feng, Zhifeng Zhang</i>	
From Survey to Application Vision: LLM Watermarking Techniques and Prospects in Scientific Scenarios	3226
<i>Chen Yucheng, Li Yang, Li Qiao, Yajiao Wang, Wang Meng, Hanyu Li</i>	
Optimization Design Method for Nets in Multi- Stage Filtration System of Nuclear Power Plant Using Cognitive Intelligence Techniques	3232
<i>PeiYan Pan, ZhiFeng Zhang, YiXiong Feng, Zhengqin Zhu, Junjie Song, JianRong Tan</i>	

A Semantic-Aware Network Intelligence Framework for Anomaly Detection using Large Language Models	3238
<i>Wei Li, Jianjun Li, Hui Shao, Junjie Li, Wei Zhang</i>	
DPDA: Decentralized Identity-Based Privacy-Preserving Data Aggregation for AIoT	3243
<i>Can Zhang</i>	
Adaptive Multi-Feature Hierarchical Framework for Generative Model Attribution	3250
<i>Ruoying Wang, Linghui Li, Xiaotian Si, Kaiguo Yuan, Zhaoyu Wang</i>	
DCARL: Decoupled-Curriculum for Adversarial Robustness Learning under Long-Tailed Distributions	3258
<i>Mingyang Chen, Linghui Li, Zhaoyu Wang, Kaiguo Yuan, Bingyu Li</i>	
OmniNova: A General Multimodal Multi-Agent Framework	3266
<i>Bingzhen Li, Zihan Wang, Pengfei Du, Yupeng Jiang</i>	
Transfer Learning based Fingerprint Database Reconstruction Scheme in Indoor Location Scenarios	3273
<i>Qian Miao, Hui Zhang, Weixin Wang, Yuanji Shi, Lihua Yang</i>	
A Dynamic Low-cost 3D Indoor Localization Algorithm Based on Error Optimal Estimation	3279
<i>Qianqian Zhu, Hui Zhang, Yuewei Zhang, Yuanji Shi, Shuyi Wang</i>	
Resource Allocation and Optimization in Low-altitude D2D Communication Networks	3285
<i>Changyuan Ji, Zongyan Li, Chen Yang, Hao Wang</i>	
MIMO Channel Modeling Based on Physics-Constrained Generative Neural Networks	3291
<i>Hanxiao Li, Hongmei Wang, Shuo Liu, Weilong Zhang</i>	
Privacy Protection Method for 3D Trajectories Integrating Semantic Information	3297
<i>Mengyao Zhang, Ding Mu, Zihan Wang, Na Fan</i>	
3D trajectory personalization privacy protection method based on multi-feature classification and spatio-temporal attention	3303
<i>Ding Mu, Mengyao Zhang, Zihan Wang, Yexiong Shang</i>	
Optimizing Spectrum Sharing in Low-Altitude Intelligent Networks: A Model-Based Reinforcement Learning Approach	3309
<i>Tianle Li, Qingyu Liu, Peixi Peng</i>	
CEE-MLIA: A Multi-Level Imbalance-Aware Framework for Contract Element Extraction	3316
<i>Bingcheng Liu, Xiao Qian, Xiuxuan Shen</i>	
Generating Structured BPMN Models from Smart Contracts Using LLMs	3322
<i>Linlin Chen</i>	
From Electronic Contracts to Smart Legal Contracts: A Template-Based Approach	3328
<i>Haoxiang Chen, Ning Zhang, Jiayue Liu</i>	
Blockchain-Enhanced Random Access in Untrusted Wireless Networks: An Evolutionary Game Analysis	3334
<i>Xinjian Li, Chang Wang, Yuwei Le, Yutong Wu, Hongwang Zhu, Jiaheng Wang, Jianjun Zhang</i>	