1. Record Nr. UNISA996668468003316

Autore	Huang De-Shuang
Titolo	Advanced Intelligent Computing Technology and Applications : 21st International Conference, ICIC 2025, Ningbo, China, July 26–29, 2025, Proceedings, Part IV / / edited by De-Shuang Huang, Wei Chen, Yijie Pan, Haiming Chen
Pubbl/distr/stampa	Singapore : , : Springer Nature Singapore : , : Imprint : Springer, , 2025
ISBN	981-9698-72-3
Edizione	[1st ed. 2025.]
Descrizione fisica	1 online resource (895 pages)
Collana	Lecture Notes in Computer Science, , 1611-3349 ; ; 15845
Altri autori (Persone)	ChenWei PanYijie ChenHaiming
Disciplina	006.3
Soggetti	Computational intelligence Computer networks Machine learning Application software Computational Intelligence Computer Communication Networks Machine Learning Computer and Information Systems Applications
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	-- Information Security -- DDos Attack Identification Based on Temporal Features. -- An Intonation-Based Black-Box Generative Adversarial Attack Method for Audio. -- RanHunter: Advancing Ransomware Detection with Channel Attention and Multi-Head Attention. -- Cellular-Snooper: A General and Real-Time Mobile Application Fingerprinting Attack in LTE Networks. -- True or False? Dually Perceiving Relevance of Source Post and Comment Flow for Rumor Detection. -- Explanation-Inspired Transferable Adversarial Attacks with Layer-Wise Increment Decomposition. -- CNN-DST-IDS: CNN and D-S Evidence Theory Based Intrusion Detection System. -- PPAGAN: A Privacy-Preserving Self-Attention GAN Framework for Image

Synthesis. -- ADPF: Adversarial Sample Detection Based on Prediction Feature. -- MvSMIA: Multi-View Source Membership Inference Attack in Federated Learning. -- RDP-FedAB: A Federated Learning Framework Balancing Privacy Protection and Model Performance. -- Transferable Adversarial Attacks via Diffusion-Based Keyword Embedding and Latent Optimization. -- Optimization of IoUT Systems: A Hierarchical Federated Transfer Learning Approach Based on UAV Computation Offloading. -- Malicious Encrypted Traffic Detection with Transformer and Dual-Layer Meta-Update Incremental Learning. -- ElevPatch: An Adversarial Patch Attack Scheme Based on YOLO11 Object Detector. -- MetaSSL-ETD: Robust Detection of Malicious Encrypted Traffic Based on Semi-Supervised Meta-Learning. -- A Steganalysis Framework for Enhancing Model Generalization Performance. -- Frequency-Aware Purification: A Black-box Defense against Backdoor Attacks. -- Stealthy Backdoors in Vertical Federated Learning. -- CTI-Shapley: An ATT&CK-Guided Enhanced Shapley Value Mechanism for Benefit Distribution in Cyber Threat Intelligence Sharing. -- Distributed Cumulative Gradient Backdoor Attack Against Federated Learning. -- MSIAA: Multi-Scale Inversion Adversarial Attack on Face Recognition. -- Leveraging Fine-Tuned Large Language Models for Device Fingerprint Extraction in IoT Security. -- MICD: Deepfake Detection with Masked Identity Consistency Detector. -- PGAE: A Perturbed Graph Autoencoder Integrating Explicit and Implicit Features for APT Detection. -- Durability-Optimized Model Poisoning Attack against Federated Learning Systems. -- Explainable Machine Learning Models for Phishing Website Detection: Enhancing Transparency and Accuracy in Cybersecurity. -- FRIFL: A Fair and Robust Incentive Mechanism for Heterogeneous Federated Learning. -- Reversible Data Hiding for 3D Mesh Models in Encrypted Domain Based on Adaptive MSB and Difference Prediction. -- FedFIP: A Personalized Federated Learning Optimization Method with Differential Privacy Protection. -- ProAnalyzer: Inferring Network Service's Fuzzing Format with Grey-box Metric. -- Research on Differential Privacy in Personalized Heterogeneous Federated Learning Based on Fisher Information Matrix. -- APFedEmb: An Adaptive and Personalized Federated Knowledge Graph Embedding Framework for Link Prediction. -- Federated Knowledge Collaborative Recommendation System with Privacy Preserving. -- Towards Reliable Detection of Malicious DNS-over-HTTPS (DoH) Tunneling Traffic under Low-quality Training Data. -- Ensemble Partitioning: A Defense Mechanism Against Membership Inference Attacks in ML Models. -- A Trusted Computing Power Network Scheduling Algorithm Based on Federated Learning. -- Secure Outsourced Matrix Multiplication of Floating Point Numbers. -- Research on Synthetic Trajectory Data Publication Resisting Location Inference Attacks Based on Differential Privacy. -- Alias6: An IPv6 Alias Resolution Technology Based on Multiple Fingerprint Features. -- Update Recovery Attacks on Two-Dimensional Encrypted Databases: Exploiting Volume Pattern Leakage in Range Queries. -- VulPelican: an LLM and Interactive Static Analysis Tool Based Vulnerability Detection Framework. -- Energy-aware Task Scheduling Using DVFS and On/Off Switching in Data Center.

Sommario/riassunto

This 20-volume set LNCS 15842-15861 constitutes - in conjunction with the 4-volume set LNAI 15862-15865 and the 4-volume set LNBI 15866-15869 - the refereed proceedings of the 21st International Conference on Intelligent Computing, ICIC 2025, held in Ningbo, China, during July 26-29, 2025. The total of 1206 regular papers were carefully reviewed and selected from 4032 submissions. This year, the conference concentrated mainly on the theories and methodologies as

well as the emerging applications of intelligent computing. Its aim was to unify the picture of contemporary intelligent computing techniques as an integral concept that highlights the trends in advanced computational intelligence and bridges theoretical research with applications. Therefore, the theme for this conference was "Advanced Intelligent Computing Technology and Applications".