1. Record Nr. UNINA9910644260203321

Titolo	Machine learning for cyber security : 4th international conference, ML4CS 2022, Guangzhou, China, December 2-4, 2022, proceedings, Part I / / edited by Yuan Xu [and four others]
Pubbl/distr/stampa	Cham, Switzerland : , : Springer, , [2023] ©2023
ISBN	3-031-20096-9
Edizione	[1st ed. 2023.]
Descrizione fisica	1 online resource (694 pages)
Collana	Lecture Notes in Computer Science, , 1611-3349 ; ; 13655
Disciplina	006.31
Soggetti	Computer security Machine learning
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Traditional Chinese Medicine Health Status Identification with Graph Attention Network -- "Flexible Task Splitting Strategy in Aircraft Maintenance Technician Scheduling Based on Swarm Intelligence" -- Privacy Preserving CSI Fingerprint Device-Free Localization -- A Novel Blockchain-MEC-based Near-domain Medical Resource Sharing Model -- Pairwise Decomposition of Directed Graphic Models for Performing Amortized Approximate Inference -- VDDL: A Deep Learning-based Vulnerability Detection Model for Smart Contracts -- "Robust Remote Sensing Scene Classification with Multi-View Voting and Entropy Ranking" -- Visualized analysis of the emerging trends of automated audio description technology -- Anomaly Detection for Multi-Time Series with Normalizing Flow -- Encrypted Transmission Method of Network Speech Recognition Information Based on Big Data Analysis -- "A Lightweight NFT Auction Protocol for Cross-chain Environment" -- "A Multi-Scale Framework for Out-of-Distribution Detection in Dermoscopic Images" -- Swarm Intelligence for Multi-objective Portfolio Optimization -- Research on Secure Cloud Storage of Regional Economic Data Network Based on Blockchain Technology -- "Data Leakage with Label Reconstruction in Distributed Learning Environments" -- Analysis Method of Abnormal Traffic of Teaching Network in Higher Vocational Massive Open Online Course Based on

Deep Convolutional Neural Network -- "Spatio-Temporal Context Modeling for Road Obstacle Detection" -- A Survey of Android Malware Detection Based on Deep Learning -- "Information Encryption Transmission Method of Automobile Communication Network Based on Neural Network" -- Explanation-Guided Minimum Adversarial Attack -- CIFD: A Distance for Complex Intuitionistic Fuzzy Set -- Security Evaluation Method of Distance Education Network Nodes Based on Machine Learning -- "MUEBA:A Multi-Model System for Insider Threat Detection" -- "Bayesian Based Security Detection Method for Vehicle CAN Bus Network" -- "Discrete Wavelet Transform-based CNN for Breast Cancer Classification from Histopathology Images" -- "Machine Learning Based Security Situation Awareness Method for Network Data Transmission Process" -- Multi-objective Hydrologic Cycle Optimization for Integrated Container Terminal Scheduling Problem -- A Method for Residual Network Image Classification with Multi-scale Feature Fusion -- "High Voltage Power Communication Network Security Early Warning and Monitoring System Based on Hmac Algorithm" -- "Large Scale Network Intrusion Detection Model Based on FS Feature Selection" -- "Research on Intelligent Detection Method of Automotive Network Data Security Based on FlexRay/CAN Gateway" -- Adversarial Attack and Defense on Natural Language Processing in Deep Learning: A Survey and Perspective -- A Novel Security Scheme for Mobile Healthcare in Digital Twin -- Construction of Security Risk Prediction Model for Wireless Transmission of Multi Axis NC Machining Data -- Spiking Neural Networks Subject to Adversarial Attacks in Spiking Domain -- Diverse Web APIs Recommendation with Privacy-preservation for Mashup Development -- Network Security Evaluation Method of College Freshmen Career Counseling Service Based on Machine Learning -- FedTDEfficiently share telemedicine data with federated distillation learning -- Increase channel attention based on Unet++ architecture for medical images -- Distributed Power Load Missing Value Forecasting with Privacy Protection -- Differentially Private Generative Model with Ratio-based Gradient Clipping -- Differential privacy protection algorithm for data clustering center -- Improved Kmeans algorithm based on privacy protection -- Symmetry Structured Analysis Sparse Coding for Key Frame Extraction -- Data Reconstruction from Gradient Updates in Federated Learning -- Natural Backdoor Attacks on Speech Recognition Models -- Boarding Pass Positioning with Jointly Multi-channel Segmentation and Perspective Transformation Correction -- AP-GCL:Adversarial perturbation on graph contrastive learning -- An Overview of Opponent Modeling for Multi-agent Competition -- Adversarial Attack and Defense on Natural Language Processing in Deep Learning: A Survey and Perspective.

Sommario/riassunto

The three-volume proceedings set LNCS 13655,13656 and 13657 constitutes the refereed proceedings of the 4th International Conference on Machine Learning for Cyber Security, ML4CS 2022, which taking place during December 2–4, 2022, held in Guangzhou, China. The 100 full papers and 46 short papers were included in these proceedings were carefully reviewed and selected from 367 submissions.