1.	Record Nr.	UNINA9910831003703321
	Titolo	Artificial Intelligence Security and Privacy : First International Conference on Artificial Intelligence Security and Privacy, AIS&P 2023, Guangzhou, China, December 3–5, 2023, Proceedings, Part II / / edited by Jaideep Vaidya, Moncef Gabbouj, Jin Li
	Pubbl/distr/stampa	Singapore : , : Springer Nature Singapore : , : Imprint : Springer, , 2024
	ISBN	981-9997-88-7
	Edizione	[1st ed. 2024.]
	Descrizione fisica	1 online resource (293 pages)
	Collana	Lecture Notes in Computer Science, , 1611-3349 ; ; 14510
	Disciplina	006.3
	Soggetti	Artificial intelligence Security systems Data protection - Law and legislation Cryptography Data encryption (Computer science) Data protection Artificial Intelligence Security Science and Technology Privacy Cryptology Security Services
	Lingua di pubblicazione	Inglese
	Formato	Materiale a stampa
	Livello bibliografico	Monografia
	Nota di contenuto	Application of lattice-based unique ring signature in blockchain transactions -- Rethinking Distribution Alignment for Inter-class Fairness -- Online Learning Behavior Analysis and Achievement Prediction with Explainable Machine Learning -- A Privacy-Preserving Face Recognition Scheme Combining Homomorphic Encryption and Parallel Computing -- A graph-based vertical federation broad learning system -- EPoLORE: Efficient and Privacy Preserved Logistic Regression scheme -- Multi-dimensional Data Aggregation Scheme without a Trusted Third Party in Smart Grid -- Using Micro Videos to Optimize Premiere Software Course Teaching -- The Design and Implementation

of Python Knowledge Graph for Programming Teaching -- An Improved Prototypical Network for Endoscopic Grading of Intestinal Metaplasia -- Secure Position-aware Graph Neural Networks for Session-based Recommendation -- Design of a Fast Recognition Method for College Students' Classroom Expression Images Based on Deep Learning -- Research on ALSTM-SVR based Traffic Flow prediction adaptive beacon message Joint control -- An Improved Hybrid Sampling Model for Network Intrusion Detection Based on Data Imbalance -- Using the SGE-CGAM Method to Address Class Imbalance Issues in Network Intrusion Detection -- A Study of Adaptive Algorithm for Dynamic Adjustment of Transmission Power and Contention Window -- Deep learning-based lung nodule segmentation and 3D reconstruction algorithm for CT images -- GridFormer: Grid foreign object detection also requires Transformer -- An Anomaly Detection and Localization Method Based on Feature Fusion and Attention -- Ensemble of Deep Convolutional Network for Citrus Disease Classification using Leaf Images -- PM2.5 Monitoring And Prediction Basing On IOT And RNN Neural Network -- An image zero watermark algorithm based on DINOv2 and multiple cycle transformation -- An image copyright authentication model based on blockchain and digital watermark.

Sommario/riassunto

This two-volume set LNCS 14509-14510, constitutes the refereed proceedings of the First International Conference on Artificial Intelligence Security and Privacy, AIS&P 2023, held in Guangzhou, China, during December 3–5, 2023. The 40 regular papers and 23 workshop papers presented in this two-volume set were carefully reviewed and selected from 115 submissions. Topics of interest include, e.g., attacks and defence on AI systems; adversarial learning; privacy-preserving data mining; differential privacy; trustworthy AI; AI fairness; AI interpretability; cryptography for AI; security applications.