1.

Record Nr.	UNINA9910831010203321
Autore	Vaidya Jaideep
Titolo	Artificial Intelligence Security and Privacy [[electronic resource]] : First International Conference on Artificial Intelligence Security and Privacy, AIS&P 2023, Guangzhou, China, December 3–5, 2023, Proceedings, Part I / / edited by Jaideep Vaidya, Moncef Gabbouj, Jin Li
Pubbl/distr/stampa	Singapore : , : Springer Nature Singapore : , : Imprint : Springer, , 2024
ISBN	981-9997-85-2
Edizione	[1st ed. 2024.]
Descrizione fisica	1 online resource (610 pages)
Collana	Lecture Notes in Computer Science, , 1611-3349 ; ; 14509
Altri autori (Persone)	GabboujMoncef LiJin
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	Fine-grained Searchable Encryption Scheme -- Fine-grained Authorized Secure Deduplication with Dynamic Policy -- Deep Multi-Image Hiding with Random Key -- Member Inference Attacks in Federated Contrastive Learning -- A network traffic anomaly detection method based on shapelet and KNN -- DFaP: Data Filtering and Purification Against Backdoor Attacks -- A Survey of Privacy Preserving Subgraph Matching Method -- The Analysis of Schnorr Multi-Signatures and the Application to AI -- Active Defense against Image Steganography -- Strict Differentially Private Support Vector Machines

with Dimensionality Reduction -- Converging Blockchain and Deep Learning in UAV Network Defense Strategy: Ensuring Data Security During Flight -- Towards Heterogeneous Federated Learning: Analysis, Solutions, and Future Directions -- From Passive Defense to Proactive Defence: Strategies and Technologies -- Research on Surface Defect Detection System of Chip Inductors Based on Machine Vision -- Multimodal fatigue detection in drivers via physiological and visual signals -- Protecting Bilateral Privacy in Machine Learning-as-a-Service: A Differential Privacy Based Defense -- FedCMK: An Efficient Privacy-Preserving Federated Learning Framework -- An embedded cost learning framework based on cumulative gradient -- An Assurance Case Practice of AI-enabled Systems on Maritime Inspection -- Research and Implementation of EXFAT File System Reconstruction Algorithm Based on Cluster Size Assumption and Computational Verification -- A Verifiable Dynamic Multi-Secret Sharing Obfuscation Scheme Applied to Data LakeHouse -- DZIP: A Data Deduplication-Compatible Enhanced Version of Gzip -- Efficient Wildcard Searchable Symmetric Encryption with Forward and Backward Security -- Adversarial Attacks against Object Detection in Remote Sensing Images -- Hardware Implementation and Optimization of Critical Modules of SM9 Digital Signature Algorithm -- Post-quantum Dropout-resilient Aggregation for Federated Learning via Lattice-based PRF -- Practical and Privacy-Preserving Decision Tree Evaluation with One Round Communication -- IoT-Inspired Education 4.0 Framework for Higher Education and Industry Needs -- Multi-agent Reinforcement Learning Based User-Centric Demand Response with Non-Intrusive Load Monitoring -- Decision Poisson: From universal gravitation to offline reinforcement learning -- SSL-ABD:An Adversarial Defense MethodAgainst Backdoor Attacks in Self-supervised Learning -- Personalized Differential Privacy in the Shuffle Model -- MKD: Mutual Knowledge Distillation for Membership Privacy Protection -- Fuzzing Drone Control System Configurations Based on Quality-Diversity Enhanced Genetic Algorithm -- KEP: Keystroke Evoked Potential for EEG-based User Authentication -- Verifiable Secure Aggregation Protocol under Federated Learning -- Electronic voting privacy protection scheme based on double signature in Consortium Blockchain -- Securing 5G Positioning via Zero Trust Architecture -- Email Reading Behavior-informed Machine Learning Model to Predict Phishing Susceptibility. .

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. .