1. Record Nr. UNINA9911047710203321

Autore	Chen Xiaofeng
Titolo	Data Security and Privacy Protection : Third International Conference, DSPP 2025, Xi'an, China, October 16–18, 2025, Proceedings, Part I / / edited by Xiaofeng Chen, Haibo Hu, Ding Wang
Pubbl/distr/stampa	Singapore : , : Springer Nature Singapore : , : Imprint : Springer, , 2026
ISBN	981-9531-82-9
Edizione	[1st ed. 2026.]
Descrizione fisica	1 online resource (811 pages)
Collana	Lecture Notes in Computer Science, , 1611-3349 ; ; 16176
Altri autori (Persone)	HuHaibo WangDing
Disciplina	005.8
Soggetti	Data protection Data protection - Law and legislation Cryptography Data encryption (Computer science) Computer security Computer networks - Security measures Data and Information Security Privacy Cryptology Security Services Principles and Models of Security Mobile and Network Security
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	-- AI and System Security. -- Boosting Transferability of Adversarial Attacks On Vision Transformer . -- DMD: Boosting Adversarial Transferability via Dynamic Momentum Decay. -- Ghosts in DBMS: Revealing the Security Impacts of Silent Fixes. -- PerTrajTree-DP: A Personalized Privacy-Preserving Trajectory Publishing Framework for Trustworthy AI Systems. -- A Code Vulnerability Detection Method Integrating Pre-trained Model and Graph Neural Network. -- Blockchain and Related Technologies. -- Covert Channels in Bitcoin: Concealing Senders via Transaction Behavior Mimicry. -- Hash Time-

Locked Contract Scheme Based on Enclave-Based Agent and Stealth Addresses. -- Smart Contract Ponzi Detection via Contract Transaction Graph. -- Evading AI-Based Detectors: A Hybrid Covert Communication Method Based on Ethereum Transaction Amount and Address. -- Hierarchical Byzantine Consensus for Election Security. -- Towards Blockchain-Enabled Cybersecurity Risk Assessment for Cyber-ship Systems. -- Spectrum Resources Privacy-preserving Allocation and Certificate Management Technology based on blockchain. -- A Blockchain-Based Framework for UAVs in an Asynchronous Network Environment. -- BCDAC: Efficient Blockchain-based Cross Domain Access Control Scheme. -- Privacy Preserving/Enhancing Technologies. -- An Efficient Private Signaling with Function Secret Sharing. -- Secure and Efficient Multi-Dimensional Task Matching in Spatial Crowdsourcing. -- PB-TPR: A Smart Grid Privacy Protection Framework for Secure Data Sharing and Efficient Aggregation. -- Efficient Ranking, Order Statistics, and Sorting under (2, 2)-Threshold Paillier. -- Personalized Secure Anonymous Traceability Mechanism with Pseudo-Random Hopping of Dynamic ID. -- A Fully Homomorphic Encryption-Based KNN Classification Scheme for Electric Vehicles Data. -- A High-Precision and Scalable Location Privacy Query System Based on FHE. -- Cryptographic Primitives. -- Secure Non-Interactive Decision Tree Evaluation via Fully Homomorphic Encryption. -- Strong Designated-Verifier zk-SNARKs. -- Short Lattice-Based Linearly Homomorphic Signatures in the Standard Model. -- Kleptographic Fountain- Leakage via a Binary Erasure Channel . -- Efficient Implementation of NTRU-based Key Encapsulation Mechanism on Embedded Platform. -- An Efficient Designated-Server Public-Key Encryption Scheme with Keyword Search based on Lattices. -- Privacy-Aware Federated Learning. -- Personalized Federated Learning with Adaptive Weight Clustering. -- FedVoD: A Robust Federated Learning Defense Strategy in Hybrid Byzantine Attacks. -- A Lightweight Data Leakage Defense Mechanism for Federated Learning based on Stochastic Gradient Masking. -- PHV-FL:A Personalized Hierarchical Verifiable Federated Learning Scheme for Maritime Target Detection. -- AI-based Security Applications and Technologies. -- Chaos: Robust Spatio-Temporal Fusion for Generalizable APT Provenance Tracing.

Sommario/riassunto

This book constitutes the proceedings of the 3rd International Conference on Data Security and Privacy Protection, DSPP 2025, held in Xi'an, China, during October 16–18, 2025. The 36 full papers and 11 short papers presented in these two volumes were carefully reviewed and selected from 105 submissions. The papers are organized in the following topical sections: Part I:AI and System Security; Blockchain and Related Technologies; Privacy Preserving/Enhancing Technologies; Cryptographic Primitives; Privacy-Aware Federated Learning; AI-based Security Applications and Technologies. Part II: AI-based Security Applications and Technologies; Cryptographic Protocols Design and Analysis; Model Security and Copyright Protection.