1. Record Nr. UNINA9910983324703321

| | |
|---|---|
| Autore | Zhang Fangguo |
| Titolo | Artificial Intelligence Security and Privacy : Second International Conference, AIS&P 2024, Guangzhou, China, December 6-7, 2024, Proceedings / / edited by Fangguo Zhang, Weiwei Lin, Hongyang Yan |
| Pubbl/distr/stampa | Singapore : , : Springer Nature Singapore : , : Imprint : Springer, , 2025 |
| ISBN | 9789819611485<br>9789819611478 |
| Edizione | [1st ed. 2025.] |
| Descrizione fisica | 1 online resource (254 pages) |
| Collana | Lecture Notes in Computer Science, , 1611-3349 ; ; 15399 |
| Altri autori (Persone) | LinWeiwei<br>YanHongyang |
| Disciplina | 006.3 |
| Soggetti | Artificial intelligence<br>Security systems<br>Data protection - Law and legislation<br>Cryptography<br>Data encryption (Computer science)<br>Data protection<br>Artificial Intelligence<br>Security Science and Technology<br>Privacy<br>Cryptology<br>Security Services |
| Lingua di pubblicazione | Inglese |
| Formato | Materiale a stampa |
| Livello bibliografico | Monografia |
| Nota di contenuto | -- BadHAR: Backdoor Attacks in Federated Human Activity Recognition Systems. -- Fully Automated Generation Mechanism of Rootfs for Specified Operating Systems under Linux. -- Anti-Side-Channel Attack Mechanisms in Blockchain Payment Channels. -- F2L: A Lightweight Focus Layer against Backdoor Attack in Federated Learning. -- Intelligent backpack based on ireless mobile technology. -- Tourism Industry Upgrading and Public Opinion Prevention Methods Based on BERTopic: A Case Study of Hotel Management. -- Privacy-Preserving Covert Channels in VoLTE via Inter-Frame Delay Modulation. -- |

Enhancing Adversarial Robustness in Object Detection via Multi-Task Learning and Class-Aware Adversarial Training. -- FedHKD: A Hierarchical Federated Learning Approach Integrating lustering and Knowledge Distillation for Non-IID Data. -- Application of Ensemble Learning Based on High-Dimensional Features in Financial Big Data. -- Collaborative Framework for Dynamic Knowledge Updating and Transparent Reasoning with Large Language Models. -- Zero-Shot Dense Retrieval based on Query Expansion. -- Lightweight Attention-CycleGAN for Nighttime-Daytime Image ransformation. -- Generative Image Steganography Based on Latent Space Vector Coding and Diffusion Model.

Sommario/riassunto

This book constitutes the refereed proceedings of the Second International Conference on Artificial Intelligence Security and Privacy, AIS&P 2024, held in Guangzhou, China, during December 6-7, 2024. The 14 full papers included in this book were carefully reviewed and selected from 47 submissions. The papers help to researchers to exchange latest research progress in all areas such as artificial intelligence, security and privacy, and their applications.