

1. Record Nr.	UNISA996664546003316
Autore	Katsikas Sokratis
Titolo	Data and Applications Security and Privacy XXXIX : 39th IFIP WG 11.3 Annual Conference on Data and Applications Security and Privacy, DBSec 2025, Gjøvik, Norway, June 23-24, 2025, Proceedings // edited by Sokratis Katsikas, Basit Shafiq
Pubbl/distr/stampa	Cham : , : Springer Nature Switzerland : , : Imprint : Springer, , 2025
ISBN	3-031-96590-6
Edizione	[1st ed. 2025.]
Descrizione fisica	1 online resource (640 pages)
Collana	Lecture Notes in Computer Science, , 1611-3349 ; ; 15722
Altri autori (Persone)	ShafiqBasit
Disciplina	005.8
Soggetti	Data protection Computers Artificial intelligence Data structures (Computer science) Information theory Database management Application software Data and Information Security Computing Milieux Artificial Intelligence Data Structures and Information Theory Database Management System Computer and Information Systems Applications
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	-- AI applications in security and privacy. -- Jibber-Jabber!: Encoding the (Un-)Natural Language of Network Devices and Applications. -- Automated Privacy Policy Analysis using Large Language Models. -- Data Chameleon:~a self-adaptive synthetic data management system. -- Operating Under Constraints: Identifying Requirements for Enhanced Cyber Resilience Management. -- Towards the Identification of Vulnerability-Fixing Code Lines in OSS Security Patches Using Lexical Code Segmentation and LLMs. -- Encrypt What Matters: Selective

Model Encryption for More Efficient Secure Federated Learning. -- Hallucination Detection in Large Language Models using Diversion Decoding. -- User and data privacy. -- Blockchain-Enhanced User Consent for GDPR-Compliant Real-Time Bidding. -- Enabling Right to be Forgotten in a Collaborative Environment using Permissioned Blockchains. -- P-EDR: Privacy-preserving Event-driven Data Release using Smart Contracts. -- Performance-Efficient Anti-fingerprinting for Privacy. -- Privacy Management in Cyber-Physical Systems: The DUCA Framework. -- Database and storage security. -- Bloom Filter Look-Up Tables for Private and Secure Distributed Databases in Web3. -- Purpose Filter: A space-efficient purpose metadata storage. -- Secure and Reliable Digital Wallets: A Threat Model for Secure Storage in eIDAS 2.0. -- Differential privacy. -- Facility Location Problem under Local Differential Privacy without Super-set Assumption. -- Can Differentially Private Fine-tuning LLMs Protect Against Privacy Attacks?. -- Attackers and attack detection. -- Metadata Assisted Supply-Chain Attack Detection for Ansible. -- Diffusion-based Adversarial Purification for Intrusion Detection. -- Feature Identification and Study of Attackers' Behaviours Using Honeypots. -- Access control & Internal Controls and Audit process. -- Supporting Delegation in Outsourced ICA Process. -- Transaction Logs in Access Control: Leveraging an Under-Utilized Data Source. -- Cryptography for security and privacy. -- The Privacy Impact of Dash Mixing Fee Payments. -- Cryptanalysis and Modification of a Variant of Matrix Operation for Randomization or Encryption (v-MORE).

Sommario/riassunto

This book constitutes the refereed proceedings of the 39th IFIP WG 11.3 Annual Conference on Data and Applications Security and Privacy XXXIX, DBSec 2025, held in Gjøvik, Norway, during June 23-24, 2025. The 19 full papers and 5 short papers included in this book were carefully reviewed and selected from 59 submissions. They were organized in topical sections as follows: AI applications in security and privacy; User and data privacy; Database and storage security; Differential privacy; Attackers and attack detection; Access control & Internal Controls and Audit process; and Cryptography for security and privacy.
