1. Record Nr. UNINA9911011655503321

Autore	Adi Kamel
Titolo	Foundations and Practice of Security : 17th International Symposium, FPS 2024, Montréal, QC, Canada, December 9–11, 2024, Revised Selected Papers, Part II / / edited by Kamel Adi, Simon Bourdeau, Christel Durand, Valérie Viet Triem Tong, Alina Dulipovici, Yvon Kermarrec, Joaquin Garcia-Alfaro
Pubbl/distr/stampa	Cham : , : Springer Nature Switzerland : , : Imprint : Springer, , 2025
ISBN	3-031-87496-X
Edizione	[1st ed. 2025.]
Descrizione fisica	1 online resource (319 pages)
Collana	Lecture Notes in Computer Science, , 1611-3349 ; ; 15533
Altri autori (Persone)	BourdeauSimon DurandChristel Viet Triem TongValérie DulipoviciAlina KermarrecYvon Garcia-AlfaroJoaquin
Disciplina	005.8
Soggetti	Data protection Computer engineering Computer networks Data and Information Security Computer Engineering and Networks Computer Communication Networks
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	-- Preserving privacy and maintaining trust for end users in a complex and numeric cyberspace. -- Another Walk for Monchi. -- An Innovative DSSE Framework: Ensuring Data Privacy and Query Verification in Untrusted Cloud Environments. -- Privacy-Preserving Machine Learning Inference for Intrusion Detection. -- Priv-IoT: Privacy-preserving Machine Learning in IoT Utilizing TEE and Lightweight Ciphers. -- Intersecting security, privacy, and machine learning techniques to detect, mitigate, and prevent threats. -- LocalIntel: Generating Organizational Threat Intelligence from Global

and Local Cyber Knowledge. -- Intelligent Green Efficiency for Intrusion Detection. -- A Privacy-Preserving Behavioral Authentication System. -- Automated Exploration of Optimal Neural Network Structures for Deepfake Detection. -- An Empirical Study of Black-box based Membership Inference Attacks on a Real-World Dataset. -- New trends of machine leaning and AI applied to cybersecurity. -- ModelForge: Using GenAI to Improve the Development of Security Protocols. -- Detecting Energy Attacks in the Battery-less Internet of Things . -- Is Expert-Labeled Data Worth the Cost? Exploring Active and Semi-Supervised Learning Across Imbalance Scenarios in Financial Crime Detection. -- ExploitabilityBirthMark: An Early Predictor of the Likelihood of Exploitation.

Sommario/riassunto

This two-volume set constitutes the refereed proceedings of the 17th International Symposium on Foundations and Practice of Security, FPS 2024, held in Montréal, QC, Canada, during December 09–11, 2024. The 28 full and 11 short papers presented in this book were carefully reviewed and selected from 75 submissions. The papers were organized in the following topical sections: Part I: Critical issues of protecting systems against digital threats,considering financial, technological, and operational implications; Automating and enhancing security mechanisms in software systems and data management; Cybersecurity and AI when applied to emerging technologies; Cybersecurity and Ethics; Cybersecurity and privacy in connected and autonomous systems for IoT, smart environments, and critical infrastructure; New trends in advanced cryptographic protocols. Part II: Preserving privacy and maintaining trust for end users in a complex and numeric cyberspace; Intersecting security, privacy, and machine learning techniques to detect, mitigate, and prevent threats; New trends of machine leaning and AI applied to cybersecurity.