1. Record Nr. UNISA996673179603316

Autore	Skopik Florian
Titolo	Availability, Reliability and Security : ARES 2025 EU Projects Symposium Workshops, Ghent, Belgium, August 11–14, 2025, Proceedings, Part I / / edited by Florian Skopik, Vincent Naessens, Bjorn De Sutter
Pubbl/distr/stampa	Cham : , : Springer Nature Switzerland : , : Imprint : Springer, , 2025
ISBN	3-032-00642-2
Edizione	[1st ed. 2025.]
Descrizione fisica	1 online resource (522 pages)
Collana	Lecture Notes in Computer Science, , 1611-3349 ; ; 15998
Altri autori (Persone)	NaessensVincent De SutterBjorn
Disciplina	005.8
Soggetti	Data protection Data and Information Security
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	5th International Workshop on Advances on Privacy Preserving Technologies and Solutions (IWAPS 2025): FL-AdvGNN: A Federated Privacy-Preserving Framework of Adversarial Graph Neural Networks -- Digital twin technology for sustainable shipping: establishing cyber-security challenges and opportunities -- Red vs. Blue Team Training Scenarios for 5G/6G Networks -- LLM-Enhanced Intrusion Detection for Containerized Applications: A Two-tier Strategy for SDN and Kubernetes Environments -- A Cyber-Resilient DICE Architecture for Resource-Constrained Devices -- NullJack: An open approach for undetectable ethernet port scanning -- Group Signatures for Secure and Reliable Industrial Data Collaboration -- Real-time digital ecosystems: Integrating Virtual Personas and Digital Twins through Microservices -- Behind Enemy Lines: Strengthening Android Malware Detection with Adversarial Training. 6th Workshop on Security, Privacy, and Identity Management in the Cloud (SECPID 2025): Novel approximations of elementary functions in zero-knowledge proofs -- Relaxing the Single Point of Failure in Quantum Key Distribution Networks: an Overview of Multi-Path Approaches -- b4M: Holistic Benchmarking for MPC -- A Cloud-based Multifactor Authentication Scheme Using Post-Quantum Cryptography and Trusted Execution Environments. First International Workshop on Secure, Trustworthy, and

Robust AI (STRAI 2025): Data Poisoning in FL: Clipping Malicious Updates -- Supporting Human-Robot Collaboration and Safety with the Proposed Explainable Neuro-symbolic Reasoning -- Towards a Metric to Assess Neural Network Resilience Against Adversarial Samples -- Evaluating Fine-Tuned LLMs for AI Text Detection. 5th International Workshop on Security and Privacy in Intelligent Infrastructures (SP2I 2025): Side-Channel Analysis of OpenVINO-based Neural Network Models -- Optimizing IoT Attack Detection in Edge AI: A Comparison of Lightweight Machine Learning and Feature Reduction Techniques -- Zero-Knowledge Proof-of-Location Protocols for Vehicle Subsidies and Taxation Compliance -- Integrating Quantum Key Distribution into Academic Network: Practical Challenges and Solutions -- Kerberos-Authenticated Classical Channel for Quantum Key Distribution: A Symmetric-Key Approach to Quantum-Safe Authentication.

Sommario/riassunto

This two-volume set LNCS 15998-15999 constitutes the proceedings of the ARES 2025 EU Projects Symposium Workshops, held under the umbrella of the 20th International conference on Availability, Reliability and Security, ARES 2025, which took place in Ghent, Belgium, during August 11-14, 2025. The 42 full papers presented in this book were carefully reviewed and selected from 92 submissions. They contain papers of the following workshops: Part I: 5th International Workshop on Advances on Privacy Preserving Technologies and Solutions (IWAPS 2025); 6th Workshop on Security, Privacy, and Identity Management in the Cloud (SECPID 2025); First International Workshop on Secure, Trustworthy, and Robust AI (STRAI 2025); 5th International Workshop on Security and Privacy in Intelligent Infrastructures (SP2I 2025). Part II: 5th workshop on Education, Training and Awareness in Cybersecurity (ETACS 2025); 5th International Workshop on Security Testing and Monitoring (STAM 2025); 8th International Workshop on Emerging Network Security (ENS 2025).