1. Record Nr. UNINA9910841865103321

Autore	Boulila Wadii
Titolo	Decision Making and Security Risk Management for IoT Environments / / edited by Wadii Boulila, Jawad Ahmad, Anis Koubaa, Maha Driss, Imed Riadh Farah
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2024
ISBN	9783031475900 3031475909
Edizione	[1st ed. 2024.]
Descrizione fisica	1 online resource (231 pages)
Collana	Advances in Information Security, , 2512-2193 ; ; 106
Altri autori (Persone)	AhmadJawad KoubaaAnis DrissMaha FarahImed Riadh
Disciplina	005.8
Soggetti	Data protection - Law and legislation Machine learning Cooperating objects (Computer systems) Privacy Machine Learning Cyber-Physical Systems
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Internet of Things Overview: Architecture, Technologies, Application, and Challenges -- IoMT Applications Perspectives: from Opportunities and Security Challenges to Cyber-Risk Management -- Cybersecurity Challenges and Implications for the Adoption of Cloud Computing and IoT: DDoS Attacks as an Example -- Implementation of the C4.5 Algorithm in the Internet of Things Applications -- Intrusion Detection Systems using Machine Learning -- Multivariate Procedure for Modeling and Prediction of Temperature in Punjab, Pakistan -- New Proposed Model for the Influence of Climate Change on the Tension Anticipation in Hospital Emergencies -- Statistical Downscaling Modeling for Temperature Prediction -- UAV-based IoT applications for action recognition -- Federated Learning for Market Surveillance -- Fake News

	in Social Media: Fake News Themes and Intentional Deception in the News and on Social Media.
Sommario/riassunto	This book contains contemporary research that outlines and addresses security, privacy challenges and decision-making in IoT environments. The authors provide a variety of subjects related to the following Keywords: IoT, security, AI, deep learning, federated learning, intrusion detection systems, and distributed computing paradigms. This book also offers a collection of the most up-to-date research, providing a complete overview of security and privacy-preserving in IoT environments. It introduces new approaches based on machine learning that tackles security challenges and provides the field with new research material that’s not covered in the primary literature. The Internet of Things (IoT) refers to a network of tiny devices linked to the Internet or other communication networks. IoT is gaining popularity, because it opens up new possibilities for developing many modern applications. This would include smart cities, smart agriculture, innovativehealthcare services and more. The worldwide IoT market surpassed $100 billion in sales for the first time in 2017, and forecasts show that this number might reach $1.6 trillion by 2025. However, as IoT devices grow more widespread, threats, privacy and security concerns are growing. The massive volume of data exchanged highlights significant challenges to preserving individual privacy and securing shared data. Therefore, securing the IoT environment becomes difficult for research and industry stakeholders. Researchers, graduate students and educators in the fields of computer science, cybersecurity, distributed systems and artificial intelligence will want to purchase this book. It will also be a valuable companion for users and developers interested in decision-making and security risk management in IoT environments.