1. Record Nr. UNINA9910633913903321

Titolo	Predictive Data Security using AI : Insights and Issues of Blockchain, IoT, and DevOps / / edited by Hiren Kumar Thakkar, Mayank Swarnkar, Robin Singh Bhadoria
Pubbl/distr/stampa	Singapore : , : Springer Nature Singapore : , : Imprint : Springer, , 2023
ISBN	981-19-6290-1
Edizione	[1st ed. 2023.]
Descrizione fisica	1 online resource (222 pages)
Collana	Studies in Computational Intelligence, , 1860-9503 ; ; 1065
Disciplina	006.3
Soggetti	Data protection Internet of things Artificial intelligence Data and Information Security Internet of Things Artificial Intelligence
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references.
Nota di contenuto	Introduction to Data Security with Machine Learning: Traditional Methods vs Recent Trends -- Data Security and Predictive Informatics: Issues, Challenges, and Opportunities -- Data Security Analytics using Machine Learning: Supervised and Unsupervised Approaches -- Data Security in Data Servers: Implementation of Security in Data Servers, Content Delivery Network Servers and Proxy Servers -- Data Security in Multimedia using AI: Perspective and Practices -- Data Security in Blockchain: Data Generation, Analysis and Predictions.
Sommario/riassunto	This contributed volume consists of 11 chapters that specifically cover the security aspects of the latest technologies such as Blockchain, IoT, and DevOps, and how to effectively deal with them using Intelligent techniques. Moreover, machine learning (ML) and deep learning (DL) algorithms are also not secured and often manipulated by attackers for data stealing. This book also discusses the types of attacks and offers novel solutions to counter the attacks on ML and DL algorithms. This book describes the concepts and issues with figures and the supporting arguments with facts and charts. In addition to that, the book provides

the comparison of different security solutions in terms of experimental results with tables and charts. Besides, the book also provides the future directions for each chapter and novel alternative approaches, wherever applicable. Often the existing literature provides domain-specific knowledge such as the description of security aspects. However, the readers find it difficult to understand how to tackle the application-specific security issues. This book takes one step forward and offers the security issues, current trends, and technologies supported by alternate solutions. Moreover, the book provides thorough guidance on the applicability of ML and DL algorithms to deal with application-specific security issues followed by novel approaches to counter threats to ML and DL algorithms. The book includes contributions from academicians, researchers, security experts, security architectures, and practitioners and provides an in-depth understanding of the mentioned issues.