1.

Record Nr.	UNINA9910427698103321
Titolo	Engineering dependable and secure machine learning systems : third international workshop, EDSMLS 2020, New York City, NY, USA, February 7, 2020, revised selected papers / / Onn Shehory, Eitan Farchi, Guy Barash, (editors)
Pubbl/distr/stampa	Cham, Switzerland : , : Springer, , [2020] Â©2020
ISBN	3-030-62144-8
Edizione	[1st ed. 2020.]
Descrizione fisica	1 online resource (IX, 141 p. 44 illus., 34 illus. in color.)
Collana	Communications in computer and information science ; ; 1272
Disciplina	006.31
Soggetti	Machine learning Artificial intelligence Computer security
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Quality Management of Deep Learning Systems -- Can Attention Masks Improve Adversarial Robustness? -- Learner-Independent Data Omission Attacks -- Extraction of Complex DNN Models: Real Threat or Boogeyman? -- Principal Component Properties of Adversarial Samples -- FreaAI: Automated extraction of data slices to test machine learning models -- Density estimation in representation space to predict model uncertainty -- Automated detection of drift in deep learning based classifiers using network embedding -- Quality of syntactic implication of RL-based sentence summarization -- Dependable Neural Networks for Safety Critical Tasks.
Sommario/riassunto	This book constitutes the revised selected papers of the Third International Workshop on Engineering Dependable and Secure Machine Learning Systems, EDSMLS 2020, held in New York City, NY, USA, in February 2020. The 7 full papers and 3 short papers were thoroughly reviewed and selected from 16 submissions. The volume presents original research on dependability and quality assurance of ML software systems, adversarial attacks on ML software systems, adversarial ML and software engineering, etc. .