Batina / Bäck / Buhan

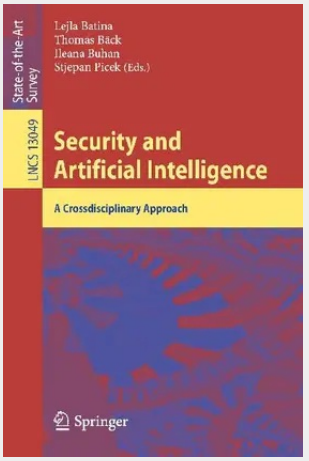
Security and Artificial Intelligence

A Crossdisciplinary Approach

AI has become an emerging technology to assess security and privacy, with many challenges and potential solutions at the algorithm, architecture, and implementation levels. So far, research on AI and security has looked at subproblems in isolation but future solutions will require sharing of experience and best practice in these domains.

The editors of this State-of-the-Art Survey invited a cross-disciplinary team of researchers to a Lorentz workshop in 2019 to improve collaboration in these areas. Some contributions were initiated at the event, others were developed since through further invitations, editing, and cross-reviewing. This contributed book contains 14 invited chapters that address side-channel attacks and fault injection, cryptographic primitives, adversarial machine learning, and intrusion detection. The chapters were evaluated based on their significance, technical quality, and relevance to the topics of security and AI, and each submission was reviewed in single-blindmode and revised.

AI has become an emerging technology to assess security and privacy, with many challenges and potential solutions at the algorithm, architecture, and implementation levels. So far, research on AI and security has looked at subproblems in isolation but future solutions will require sharing of experience and best practice in these domains.The editors of this State-of-the-Art Survey invited a cross-disciplinary team of researchers to a Lorentz workshop in 2019 to improve collaboration in these areas. Some contributions were initiated at the event, others were developed since through further invitations, editing, and cross-reviewing. This contributed book contains 14 invited chapters that address side-channel attacks and fault injection, cryptographic primitives, adversarial machine learning, and intrusion detection. The chapters were evaluated based on their significance, technical quality, and relevance to the topics of security and AI, and each submission was reviewed in single-blindmode and revised.



90,94 €
84,99 € (zzgl. MwSt.)

Lieferfrist: bis zu 10 Tage

Artikelnummer: 9783030987947
Medium: Buch
ISBN: 978-3-030-98794-7
Verlag: Springer
Erscheinungstermin: 08.04.2022
Sprache(n): Englisch
Auflage: 1. Auflage 2022
Serie: Lecture Notes in Computer Science
Produktform: Kartoniert
Gewicht: 563 g
Seiten: 361
Format (B x H): 155 x 235 mm

Kundenservice Verlag Dr. Otto Schmidt KG
Neumannstraße 10, 40235 Düsseldorf | kundenservice@otto-schmidt.de | 0221-93738-997 (Inland)