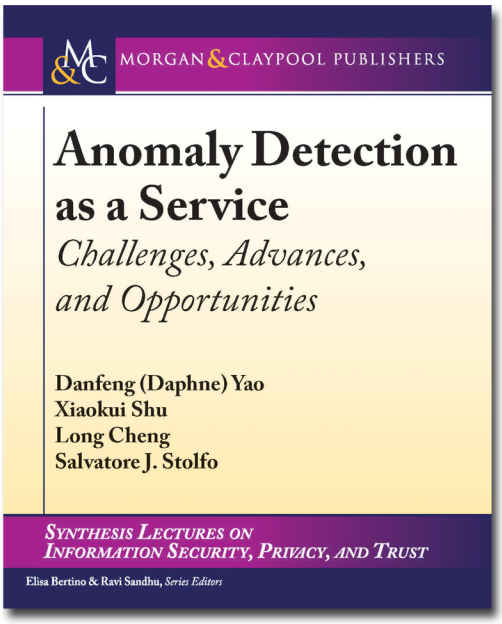
Advancing the real-world adoption and deployment of anomaly detection technologies.



Anomaly Detection as a Service

Challenges, Advances, and Opportunities

Danfeng (Daphne) Yao, *Virginia Tech*
Xiaokui Shu, *IBM Research*
Long Cheng, *Virginia Tech*
Salvatore J. Stolfo, *Columbia University*

Paperback ISBN: 9781681731094 • eBook ISBN: 9781681731100
Hardcover ISBN: 9781681732428
Published October, 2017 • 196 pages
Paperback: $69.95 • eBook: $55.96 • Combo: $87.44
Hardcover: $94.95 • Hardcover Combo: $118.69

Anomaly detection has been a long-standing security approach with versatile applications, ranging from securing server programs in critical environments, to detecting insider threats in enterprises, to anti-abuse detection for online social networks. Despite the seemingly diverse application domains, anomaly detection solutions share similar technical challenges, such as how to accurately recognize various normal patterns, how to reduce false alarms, how to adapt to concept drifts, and how to minimize performance impact. They also share similar detection approaches and evaluation methods, such as feature extraction, dimension reduction, and experimental evaluation.

The main purpose of this book is to help advance the real-world adoption and deployment of anomaly detection technologies, by systematizing the body of existing knowledge on anomaly detection. This book is focused on data-driven anomaly detection for software, systems, and networks against advanced exploits and attacks, but also touches on a number of applications, including fraud detection and insider threats. We explain the key technical components in anomaly detection workflows, give in-depth description of the state-of-the-art data-driven anomaly-based security solutions, and more importantly, point out promising new research directions. This book emphasizes on the need and challenges for deploying service-oriented anomaly detection in practice, where clients can outsource the detection to dedicated security providers and enjoy the protection without tending to the intricate details.

CONTENTS