2024 IEEE Conference on Secure and Trustworthy Machine Learning (SaTML 2024)

Toronto, Ontario, Canada
9 – 11 April 2024

IEEE

IEEE Catalog Number: CFP24BT6-POD
ISBN: 979-8-3503-4951-1

****** This is a print representation of what appears in the IEEE Digital Library. Some format issues inherent in the e-media version may also appear in this print version.***

IEEE Catalog Number: CFP24BT6-POD
ISBN (Print-On-Demand): 979-8-3503-4951-1
ISBN (Online): 979-8-3503-4950-4

Additional Copies of This Publication Are Available From:

Curran Associates, Inc
57 Morehouse Lane
Red Hook, NY 12571 USA
Phone: (845) 758-0400
Fax: (845) 758-2633
E-mail: curran@proceedings.com
Web: www.proceedings.com

2024 IEEE Conference on Secure and Trustworthy Machine Learning (SaTML)

SaTML 2024

Table of Contents

Session A: Privacy

Session B: Fairness

Session C: Verifying/Certifying Properties of ML Systems

Session D: Training-Time Integrity (backdoor Attacks, etc.)

Session E: Inference-Time Integrity (adversarial Examples, etc.)

Session F: Collaborative Learning

Session G: Patching

Session H: Auditing

Session I: Forensic Analysis of ML Systems