JSAIT IEEE Journal on Selected areas in Information Theory

Information-Theoretic Methods for Trustworthy and Reliable Machine Learning

Call for papers

Over the past decade, machine learning (ML), that is the process of enabling computing systems to take data and churn out decisions, has been enabling tremendously exciting technologies. Such technologies can assist humans in making a variety of decisions by processing complex data to identify patterns, detect anomalies, and make inferences. At the same time, these automated decision-making systems raise questions about security and privacy of user data that drive ML, fairness of the decisions, and reliability of automated systems to make complex decisions that can affect humans in significant ways. In short, how can ML models be deployed in a responsible and trustworthy manner that ensures fair and reliable decision-making? This requires ensuring that the entire ML pipeline assures security, reliability, robustness, fairness, and privacy. Information theory can shed light on each of these challenges by providing a rigorous framework to not only quantify these desirata but also rigorously evaluate and provide assurances. From its beginnings, information theory has been devoted to a theoretical understanding of the limits of engineered systems. As such, it is a vital tool in guiding machine learning advances.

We invite previously unpublished papers that contribute to the fundamentals, as well as the applications of information- and learning-theoretic methods for secure, robust, reliable, fair, private, and trustworthy machine learning. Exploration of such techniques to practical systems is also relevant.
Topics of interest include, but are not limited to,

- Theory and practice of differential privacy
- Secure and/or private distributed/federated learning
- Information-theoretic foundations of fairness including measures and methodologies
- Analysis of auditing mechanism of fair and/or private algorithms
- Exploring information-theoretic guarantees for synthetic data generation methods
- Synthetic data methods with privacy guarantees
- Applications of machine learning to coding and communications fundamental limits
- Guarantees on ML-based communication and coding systems
- Information-theoretic guarantees on machine learning generalization
- Formal analysis and guarantees for machine learning with adversaries
- Role of information theory in advancing explainable machine learning
- Online, active, and Bayesian learning through the lens of information theory

Lead Guest Editors:
Lalitha Sankar, Arizona State University, USA
Oliver Kosut, Arizona State University, USA

Senior Editor: Alon Orlitsky

Guest Editors:
Flavio Calmon, Harvard, USA Ayfer Ozgur, Stanford, USA
Lele Wang, University of British Columbia, Canada Ofer Shayevitz, Tel-Aviv University, Israel
Parastoo Sadeghi, University of New South Wales, Australia

Important Dates:
Manuscript Due: October 22, 2023 ←– **NEW DEADLINE!!**
Acceptance Notification: April 15, 2024
Expected Publication Date: June 1, 2024

Submission Guidelines: The papers will be peer-reviewed according to standard IT Society peer review procedures. The reviewers will be selected from the pool of established researchers working in the areas covered by the submitted papers, including, but not limited to security and privacy of information and learning systems, federated and distributed learning, information-theoretic methods for algorithmic fairness, adversarial machine learning, and active and online learning. Prospective authors should prepare their papers following regular submission guidelines of the IEEE Journal on Selected Areas in Information Theory (see https://www.itsoc.org/jsait/author-information).
Manuscript Submission Website: https://mc.manuscriptcentral.com/jsait-ieee