Prakhar Ganesh

COMPUTER SCIENCE · PHD STUDENT

McGill University | Quebec Al Institute (Mila)

<u>Research Interests</u>: I am interested in the challenges that arise in AI when moving from the sandbox to the real world, primarily at the intersection of multiplicity, fairness, privacy, and security, focusing on uncovering the learning dynamics of neural networks.

Education

McGill University | Quebec AI Institute (Mila)

PHD COMPUTER SCIENCE (THESIS) | ADVISOR: PROF GOLNOOSH FARNADI

Jan 2024 - Present

National University of Singapore (NUS)

MASTER OF COMPUTING (AI SPECIALISATION) | ADVISOR: PROF REZA SHOKRI

Aug 2021 - Mar 2023

Indian Institute of Technology Delhi (IITD)

BACHELOR OF TECHNOLOGY IN COMPUTER SCIENCE AND ENGINEERING

Aug 2015 - May 2019

Work Experience_

NATIONAL UNIVERSITY OF SINGAPORE (NUS) RESEARCH INTERN	Jan 2023 - Apr 2023
ALVISUAL AI ENGINEER (INTERN)	Jan 2022 - Mar 2022
Advanced Digital Sciences Center (ADSC) Research Engineer	Jun 2019 - July 2021
Krida.AI Engineer (Intern)	Jan 2019 - May 2019
WEALTHNET ADVISORS ANALYST (INTERN)	May 2018 - July 2018

Publications

Different Horses for Different Courses: Comparing Bias Mitigation Algorithms in ML

[SPOTLIGHT PRESENTATION] WORKSHOP ON ALGORITHMIC FAIRNESS THROUGH THE LENS OF METRICS AND EVALUATION, NEURIPS 2024 Prakhar Ganesh*, Usman Gohar*, Lu Cheng, Golnoosh Farnadi

Towards More Realistic Extraction Attacks: An Adversarial Perspective

[Non-archival] Workshop on Privacy in Natural Language Processing, ACL 2024 Yash More*, Prakhar Ganesh*, Golnoosh Farnadi

The Data Minimization Principle in Machine Learning

[CONTRIBUTED TALKS] [NON-ARCHIVAL] WORKSHOP ON REGULATABLE ML, NEURIPS 2024

Prakhar Ganesh, Cuong Tran, Reza Shokri, Ferdinando Fioretto

An Empirical Investigation into Benchmarking Model Multiplicity for Trustworthy Machine Learning: A Case Study on Image Classification

IEEE/CVF WINTER CONFERENCE ON APPLICATIONS OF COMPUTER VISION (WACV), 2024

Prakhar Ganesh

On The Impact of Machine Learning Randomness on Group Fairness

 $\textbf{[Best Paper Award]} \ \mathsf{ACM} \ \mathsf{Conference} \ \mathsf{on} \ \mathsf{Fairness}, \mathsf{Accountability} \ \mathsf{and} \ \mathsf{Transparency} \ \mathsf{(FAccT)}, 2023$

Prakhar Ganesh, Hongyan Chang, Martin Strobel, Reza Shokri

YOLO-ReT: Towards High Accuracy Real-time Object Detection on Edge GPUs

 ${\sf IEEE/CVF}\ {\sf Winter}\ {\sf Conference}\ {\sf on}\ {\sf Applications}\ {\sf of}\ {\sf Computer}\ {\sf Vision}\ ({\sf WACV}), {\tt 2022}$

Prakhar Ganesh*, Yao Chen*, Yin Yang, Deming Chen, Marianne Winslett

HiKonv: High Throughput Quantized Convolution With Novel Bit-wise Management and Computation

ASIA AND SOUTH PACIFIC DESIGN AUTOMATION CONFERENCE (ASP-DAC), 2022

Yao Chen*, Xinheng Liu*, **Prakhar Ganesh**, Junhao Pan, Jinjun Xiong, Deming Chen

Compressing Large-Scale Transformer-Based Models: A Case Study on BERT

Transactions of the Association for Computational Linguistics (TACL), 2021

Prakhar Ganesh, Yao Chen, Xin Lou, Mohd. Ali Khan, Yin Yang, Hassan Sajjad, Preslav Nakov, Deming Chen, Marianne Winslett

Learning-based Detection and Characterization of Time Delay Attack in Cyber-Physical Systems

IEEE TRANSACTIONS ON SMART GRID (TSG), 2021

Prakhar Ganesh, Xin Lou, Yao Chen, Rui Tan, David K.Y. Yau, Deming Chen, Marianne Winslett

Assessing and Mitigating the Impact of Time Delay Attack: Case Studies for Power Grid Controls

IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS (JSAC), 2020

Xin Lou, Cuong Tran, Rui Tan, David K.Y. Yau, Zbigniew T. Kalbarczyk, Ambarish Kumar Banerjee, Prakhar Ganesh

Invited Talks

- Oct 2024 Responsible AI Week, Quebec AI Institute (Mila), The Curious Case of Arbitrariness in Machine Learning
- Jan 2024 Saarland University, On The Impact of Machine Learning Randomness on Model Fairness
- May 2023 Quebec AI Institute (Mila), On The Impact of Machine Learning Randomness on Model Fairness

Awards and Scholarships

- 2024 Travel Grant, IAPP Privacy Security Risk (PSR) Student Scholar program
- 2024 Travel Grant, AAAI/ACM Conference on AI, Ethics, and Society (AIES) Student Program
- 2024 **Travel Grant,** ACM Conference on Fairness, Accountability and Transparency (FAccT) Doctoral Consortium
- 2024 **Doctoral Research Scholarship**, Fonds de recherche du Québec Nature et Technologies (FRQNT)
- 2024 Graduate Research Enhancement And Travel (GREAT) Award, McGill University
- 2024 Excellence Scholarship EDI in Research Category, Mila EDI Scholarship Program
- 2024 **Graduate Excellence Award**, McGill University
- 2023 **Graduate Scholarship**, Prof. Golnoosh Farnadi, Quebec Al Institute (Mila)
- 2023 Best Paper Award, ACM Conference on Fairness, Accountability and Transparency (FAccT)
- 2023 Travel Grant, ACM Conference on Fairness, Accountability and Transparency (FAccT)
- 2022 Winner, 8-Bit Bias Bounty Competition Supervised Learning Track

Teaching and Mentorship Experience

- 2025 **Teaching Assistant**, Winter-COMP-598: Responsible AI, McGill University
- 2025 **Bridge Mentor**, CSGS x CSUS Bridge Mentorship Program, McGill University
- 2024 **Teaching Assistant**, Fall-COMP-370: Introduction to Data Science, McGill University
- 2024 Instructor, Indigenous Pathfinders in Al
- 2024 **Teaching Assistant**, Al4Good Lab: Summer ML Bootcamp
- 2024 **Coding Mentor**, Girls Who Code Hackathon
- 2024 **Teaching Assistant**, Winter-COMP-553: Algorithmic Game Theory, McGill University

Professional and Volunteer Service

Area Chair ACL Rolling Reviews (ARR)	Dec, 2024
PEER REVIEWER INTERNATIONAL CONFERENCE ON MACHINE LEARNING (ICML)	2025
PEER REVIEWER INTERNATIONAL CONFERENCE ON ARTIFICIAL INTELLIGENCE AND STATISTICS (AISTATS)	2025
PEER REVIEWER INTERNATIONAL CONFERENCE ON LEARNING REPRESENTATIONS (ICLR)	2025
PEER REVIEWER WINTER CONFERENCE ON APPLICATION OF COMPUTER VISION (WACV)	2025, 2024, 2022, 2021
PEER REVIEWER, ETHICS REVIEWER NEURAL INFORMATION PROCESSING SYSTEMS (NEURIPS)	2024
Volunteer, Peer Reviewer ACM Conference on Fairness, Accountability and Transparency (FAccT)	2024
PEER REVIEWER, ETHICS REVIEWER ACL ROLLING REVIEWS (ARR)	Feb and June, 2024
PEER REVIEWER ALGORITHMIC FAIRNESS THROUGH THE LENS OF METRICS AND EVALUATION (AFME) WORKSHOP, NEURIPS	2024
PEER REVIEWER RESPONSIBLE GENERATIVE AI WORKSHOP, CVPR	2024
ETHICS REVIEWER NEURAL INFORMATION PROCESSING SYSTEMS (NEURIPS)	2023
PEER REVIEWER ALGORITHMIC FAIRNESS THROUGH THE LENS OF TIME (AFT) WORKSHOP, NEURIPS	2023
PEER REVIEWER AAAI CONFERENCE ON ARTIFICIAL INTELLIGENCE (AAAI)	2021

Preprints/Manuscripts

Free Lunch for Co-Saliency Detection: Context Adjustment

ARXIV PREPRINT ARXIV:2108.02093

Lingdong Kong, Prakhar Ganesh, Tan Wang, Junhao Liu, Le Zhang, Yao Chen

Restructuring Conversations using Discourse Relations for Zero-shot Abstractive Dialogue Summarization

ARXIV PREPRINT ARXIV:1902.01615

Prakhar Ganesh, Saket Dingliwal

VLSTM: Very Long Short-Term Memory Networks for High-Frequency Trading

ARXIV PREPRINT ARXIV:1809.01506

Prakhar Ganesh, Puneet Rakheja

Nucl2Vec: Local alignment of DNA sequences using Distributed Vector Representation

BIORXIV PREPRINT DOI:10.1101/401851

Prakhar Ganesh, Gaurav Gupta, Shubhi Saini, Kolin Paul