RAKSHIT NAIDU NEMAKALLU

Email ⋄ LinkedIn ⋄ Website ⋄ Google Scholar

OBJECTIVE

My research interests hover around topics in Ethical Machine Learning (ML), Trustworthy/Responsible Artificial Intelligence (AI), and AI for societal good. I'm interested in creating applications that have a direct impact on society through my research.

EDUCATION

Doctor of Philosophy (Ph.D.) in Computational Science and Engineering, Georgia Institute of Technology
2023 - (Expected) 2028

Master of Science (M.Sc.) in Information Technology (Privacy Engineering), Carnegie Mellon University
2021 - 2022
Selected Courses: Ethics in Machine Learning, Foundations of Privacy, Privacy Policy, Law and Technology (PPLT) and ML with Large Datasets

Bachelor of Technology (B.Tech.) in Computer Science and Engineering, Manipal Institute of Technology
2017 - 2021
Minor in Computational Mathematics
Selected Courses: Computational Linear Algebra, Distributed and Cloud Computing, Graph Theory and Matrices.

EXPERIENCE

Graduate Research Intern — Apr 2023 - July 2023
Carnegie Mellon University — *Pittsburgh, PA, USA*

- Worked with Prof. Hoda Heidari as a Research Assistant in the Machine Learning Department (MLD) at CMU.
- My responsibilities entailed of collecting, assimilating, and analyzing both qualitative and quantitative data from prior academic publications, with the goal of creating a tool that offers a pipeline-aware view of Fairness for Machine Learning to researchers and practitioners.
- Outcome – Accepted as oral talk at ACM EAAMO'23 and NeurIPS'23 tutorial (Toward Operationalizing Pipeline-aware ML Fairness).

Visiting Research Scholar — Jun 2022 - Aug 2022
Syracuse University — *Syracuse, NY, USA*

- Worked with Prof. Ferdinando Fioretto on topics related to Differential Privacy and Fairness in AI.
- Outcome – Accepted as Spotlight Talk at NeurIPS'22 (Pruning has a disparate impact on model accuracy).

Application Engineering Intern — Jan 2021 - Jul 2021
BlackRock — *Gurugram, India (Remote)*

- Part of the Client-End Fund Reporting Team. Improved test coverage on FRED (Factsheet Reporting Engine and Distribution) and fixed code issues, blockers and bugs.
- Received an honourable mention for our internal hackathon project on "BlackRock's Cultural Heatmap" which provides a forum for both employees (to assess their mental and cultural well-being) and managers (to maintain a cultural pulse throughout the organization).

PUBLICATIONS & PROJECTS

Are Chatbots Ready for Privacy-Sensitive Applications? An Investigation into Input Regurgitation and Prompt-Induced Sanitization — Link
*Aman Priyanshu, Supriti Vijay, Ayush Kumar, **Rakshit Naidu**, Fatemehsadat Mireshghallah*
(*Under Review*)

Toward Operationalizing Pipeline-aware ML Fairness: A Research Agenda for Developing Practical Guidelines and Tools Link
*Emily Black, **Rakshit Naidu**, Rayid Ghani, Kit Rodolfa, Daniel Ho, Hoda Heidari*
(*Accepted at ACM Conference on Equity and Access in Algorithms, Mechanisms, and Optimization (EAAMO), 2023 (archival)*)
★ Oral Presentation (~18% acceptance rate)
★ NeurIPS'23 tutorial

Can Causal (or Counterfactual) Representations benefit from Quantum Computing? Link
***Rakshit Naidu**, Daniel Justice*
(*Accepted as an extended abstract at Algorithmic Fairness through the Lens of Causality and Privacy (AFCI) workshop at NeurIPS'22*)

Pruning has a disparate impact on model accuracy Link
*Cuong Tran, Ferdinando Fioretto, Jung-Eun Kim, **Rakshit Naidu***
(*Accepted at NeurIPS'22*)
★ Spotlight Lightning Talk (~3% acceptance rate)
★ Nomination for Best Paper Award

Fair Context-Aware Privacy Threat Modelling Link
*Saswat Das, **Rakshit Naidu***
(*Presented at Privacy Threat Modeling (PTM) workshop at USENIX-SOUPS'22*)

Can Causal (and Counterfactual) Reasoning improve Privacy Threat Modelling? Link
***Rakshit Naidu**, Navid Kagalwalla*
(*Presented at Privacy Threat Modeling (PTM) workshop at USENIX-SOUPS'22*)

Efficient Hyperparameter Optimization for Differentially Private Deep Learning Link
*Aman Priyanshu, **Rakshit Naidu**, Fatemehsadat Mireshghallah, Mohammad Malekzadeh*
(*Accepted at PPML workshop at ACM CCS'21 and as a poster at IEEE-S&P'21*)

Privacy Enabled Financial Text Classification using Differential Privacy and Federated Learning Link
Priyam Basu, Tiasa Singha Roy*, **Rakshit Naidu**, Zumrut Muftuoglu*
(*Accepted at Economics and Natural Language Processing (ECONLP) workshop at EMNLP'21*)

Benchmarking Differential Privacy and Federated Learning for BERT models Link
Priyam Basu, Tiasa Singha Roy*, **Rakshit Naidu**, Zumrut Muftuoglu, Sahib Singh, Fatemehsadat Mireshghallah*
(*Accepted at Machine Learning for Data: Automated Creation, Privacy, Bias (ML4Data) workshop at ICML'21*)

Towards Quantifying Carbon Emissions of Differentially Private Machine Learning Link
Rakshit Naidu*, *Harshita Diddee*, Ajinkya Mulay*, Aleti Vardhan, Krithika Ramesh, Ahmed Zamzam*
(*Accepted at Socially Responsible Machine Learning (SRML) workshop at ICML'21*)

DP-SGD vs PATE: Which Has Less Disparate Impact on Model Accuracy? Link
Archit Uniyal, **Rakshit Naidu***, Sasikanth Kotti, Patrik Joslin Kenfack, Sahib Singh, Fatemehsadat Mireshghallah, Andrew Trask*
(*Accepted at ML4Data workshop at ICML'21 and PPML workshop at ACM CCS'21. And also as a poster at IEEE-S&P'21*)

FedPerf: A Practitioners' Guide to Performance of Federated Learning Algorithms Publication
Ajinkya Mulay, Baye Gaspard*, **Rakshit Naidu***, Santiago Gonzalez-Toral*, Vineeth S*, Tushar Semwal*, Ayush Manish Agrawal*
(*Accepted for publication at PMLR*)

When Differential Privacy Meets Interpretability: A Case Study Link — Poster
Rakshit Naidu*, *Aman Priyanshu*, Aadith Kumar, Sasikanth Kotti, Haofan Wang, Fatemehsadat Mireshghallah*
(*Accepted as extended abstract at Responsible Computer Vision (RCV) workshop at CVPR'21; full paper accepted at Privacy-Preserving Machine Learning (PPML) workshop at ACM CCS'21*)

Improved variants of Score-CAM via Smoothing and Integrating Poster

***Rakshit Naidu**, Soumya Snigdha Kundu, Ankita Ghosh, Yash Maurya, Shamanth R Nayak K, Joy Michael, Haofan Wang*

(*Accepted as extended abstract at Responsible Computer Vision (RCV) workshop at CVPR'21*)

FedPandemic: A Cross-Device Federated Learning Approach Towards Elementary Prognosis of Diseases During a Pandemic Link

*Aman Priyanshu, **Rakshit Naidu***

(*Accepted at Distributed and Private Machine Learning (DPML) and Machine Learning for Preventing and Combating Pandemics (MLPCP) workshops at ICLR'21*)

SS-CAM: Smoothed Score-CAM for sharper visual feature localization Link

We introduce Smoothing to the Score-CAM algorithm, which is a state-of-the-art CAM algorithm. Smoothing allows us to capture more features of the focused object in the image, which leads to better visually attributed results.

IS-CAM: Integrated Score-CAM for axiomatic-based explanations Link

We borrow the idea of integration from "IntegratedGrad" and combine it with Score-CAM to conduct faithfulness evaluations. IS-CAM performs better than SS-CAM and Score-CAM in terms of faithfulness evaluations, considering the VGG-16 as our baseline model.

TeleVital: Enhancing the quality of contactless health assessment Paper — News

Our team came 2nd in a pan-Indian hackathon called #CODE19 and won $5000 for this solution to detect vitals from the webcam itself, thereby promoting remote diagnosis during COVID-19. I worked on the Respiratory rate calculations via webcam and was responsible for documenting the entire project for presenting at the hackathon.

AWARDS & PROFESSIONAL SERVICES

- Our team (Emily, Hoda, Kit, Rayid, Daniel and I) will be presenting a NeurIPS'23 tutorial called "AI Governance & Accountability for Machine Learning: Existing Tools, Ongoing Efforts & Future Directions", based on our EAAMO'23 paper! Congratulations to everyone involved!
- Received a travel grant worth $750 to attend and present our paper (also at the Doctoral Consortium) at ACM Conference on Equity and Access in Algorithms, Mechanisms, and Optimization (EAAMO) 2023 conference.
- Program Committee Member/Reviewer at AAAI'24 and Privacy-Preserving AI (PPAI-24) workshop at AAAI-24
- Reviewer at the XAI in Action: Past, Present, and Future Applications workshop at NeurIPS'23
- Reviewer at the Algorithmic Fairness through the Lens of Causality and Privacy workshop at NeurIPS'22, NeurIPS'23
- Recipient of the Thomas H. Johnson Fellowship award for the academic year 2023-24.
- Teaching Assistant Quantum Computing Theory and Lab (11-860), Programming Quantum Computers (17617-A1), Quantum Circuit Mappings (17-620)
- Served on the Program Committee at the GenLaw workshop @ ICML'23
- Reviewer and Ethics Reviewer at NeurIPS'23
- Attended Secure and Trustworthy ML (SaTML) 2023 conference on a travel grant worth $1000.
- Talk at Comcast Cybersecurity team (headquartered in Philadelphia, PA) on "Context-Aware Privacy Threat Modeling". The same talk was also delivered at the Privacy Threat Modeling workshop at SOUPS 2022.
- Served on the Program Committee as a reviewer at PPAI-AAAI'22, PPAI-AAAI'23.
- TEDxMAHE Countdown 2020 Speaker on *Federated Learning for Climate Change.* Event Link — Talk
- Manipal Conclave 2020 Student Speaker on *Privacy for ML.* Memento

- Poster Presented at PyCon India 2019 on *Secure and Private AI with PySyft*. Poster
  Volunteered at PyCon India 2020.

EXTRA-CURRICULAR ACTIVITIES

- Played for the CMU Badminton team in the Fall 2022 Eastern Collegiate MidAtlantic Conf (Badminton Tournament Regionals) held at University of Maryland, College Park in October 2022.
- Finished a full marathon (42 km) at Manipal Marathon 2020 with a timing of 6 hours and 33 minutes. Certificate