

# RAKSHIT NAIDU

[Email](#) ◇ [LinkedIn](#) ◇ [Website](#)

## OBJECTIVE

---

My research interests hover around the intersection of Machine Learning, Privacy and Cryptography. I hope to work on reliable and robust privacy designs for the societal good.

## EDUCATION

---

**Master of Science in Information Technology (Privacy Engineering)**, Carnegie Mellon University  
Expected 2022

Courses: Foundations of Privacy, Privacy Policy, Law and Technology (PPLT) and Current Topics in Privacy Seminar.

**Bachelor of Computer Science and Engineering**, Manipal Institute of Technology 2017 - 2021  
Minor in Computational Mathematics

Courses: Computational Linear Algebra, Distributed and Cloud Computing, Graph Theory and Matrices, MATLAB.

## EXPERIENCE

---

**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).

**Research Engineer** Mar 2020 - Present  
OpenMined *Remote*

- Collaborating on projects involving Differential Privacy, Federated Learning and Privacy-Preserving Machine Learning protocols under a Research Scientist at OpenMined.

**R&D Intern** Jun 2018 - Jul 2018  
Procreate Techno Systems *Hyderabad, India*

- Demonstrated an alternative approach for solving Speaker Identification (implemented the K-Means Clustering algorithm). The former approach used Gaussian Mixture Models(GMMs) for Speaker Identification.

**Mathematics and Marketing Intern** Jun 2018 - Jul 2018  
Sciensation India *Hyderabad, India*

- Mentored young students in a Socratic Dialogue competition.
- Evangelized research-based learning to parents and kids. I was part of the Marketing team where I had to attend fairs to interact with prospective students/parents. We posed the classic Tower of Hanoi problem to the kids and asked them to arrange the blocks under a specified time limit.

## PROJECTS & PUBLICATIONS

---

**Shamir.jl** An implementation of Shamir’s Secret Sharing protocol in Julia. [Link](#)

Shamir’s Secret Sharing scheme allows  $t$  out of  $n$  parties to recover the secret using Polynomial functions. If there are  $k$  parties (where  $k < t$ ) in the protocol, they cannot recover the secret.

**DiffPrivacy.jl** A library to implement Differential Privacy techniques over statistical databases in Julia (Under Development). [Link](#)

Differential privacy allows on to publicly share information about a dataset by describing the patterns of groups within the dataset while preserving information about individuals in the dataset. As of now, I have included *Sensitivity* functions in this package. I hope to include Bounded functions soon.

### **Efficient Hyperparameter Optimization for Differentially Private Deep Learning**

[Preprint](#)

We study three different hyperparameter optimization approaches for DP-SGD to achieve the best privacy-utility tradeoffs. (Under Review)

### **Benchmarking Differential Privacy and Federated Learning for BERT models**

[Preprint](#)

We benchmark BERT-based models with DP and FL on two Twitter datasets (Depression and Sexual harassments). We provide open source implementations for the same to accelerate Private NLP research. (Accepted at [ML4Data](#) workshop at ICML'21)

### **Towards Quantifying Carbon Emissions of Differentially Private Machine Learning**

[Preprint](#)

We quantify carbon emissions for DP-SGD in three different environments : NLP (News Classification), CV (MNIST Digit Classification) and RL (Cartpole problem). (Accepted at [SRML](#) workshop at ICML'21)

### **DP-SGD vs PATE: Which Has Less Disparate Impact on Model Accuracy?**

[Preprint](#)

We compare DP-SGD with PATE, another DP-based approach in terms of Fairness. We infer that as PATE uses a teacher-student setup where disjoint data is distributed among the teachers, it suffers less disparity than DP-SGD (due to diversity in training). (Accepted at [ML4Data](#) workshop at ICML'21)

### **FedPerf: A Practitioners' Guide to Performance of Federated Learning Algorithms**

[Publication](#)

I worked with this team on extending their NeurIPS short paper with the Stragglers and Robustness experiments. We propose an empirical investigation on four prominent FL algorithms to discover the relation between the FL System Parameters (FLSPs) and their performance. (Accepted for publication at [PMLR](#))

### **When Differential Privacy Meets Interpretability: A Case Study**

[Preprint](#) — [Poster](#)

We investigate the tradeoffs between Differentially-Private SGD (DP-SGD) and Interpretability specifically through CAMs on the APTOS dataset. (Accepted as extended abstract at [RCV](#) workshop at CVPR'21)

### **Improved variants of Score-CAM via Smoothing and Integrating**

[Poster](#)

We improve Score-CAM by adding smoothing and integration functions as suggested in the SmoothGrad and IntegratedGrad papers respectively. (Accepted as extended abstract at [RCV](#) workshop at CVPR'21)

### **FedPandemic: A Cross-Device Federated Learning Approach Towards Elementary Prognosis of Diseases During a Pandemic (2021)**

[Preprint](#)

We come up with a simple noise algorithm (inspired by Randomized Response and integrated with Federated Learning) to retrieve prominent COVID-19 symptoms in a privacy-preserving fashion. We simulate this protocol in four different scenarios and also experiment with Differential Privacy (DP) guarantees of our algorithm. (Accepted at [DPML](#) and [MLPCP](#) workshops at ICLR'21)

### **SS-CAM: Smoothed Score-CAM for sharper visual feature localization**

[Preprint](#)

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**

[Preprint](#)

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.

## CERTIFICATIONS

---

**Neural Networks and Deep Learning** offered by deeplearning.ai on Coursera.

[Certificate](#)

**Number Theory and Cryptography** offered by UCSD on Coursera.

[Certificate](#)

**Mathematics for Machine Learning: Linear Algebra** offered by ICL on Coursera.

[Certificate](#)

## EXTRA-CIRRICULAR ACTIVITIES

---

- 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.
- Core Committee Member of the Linux Users' Group, Manipal(LUGM).
- Open Source Contributor at Python Pandas, OpenMined's PySyft, Julia.
- Campus Ambassador and Beta Tester for Coursera.
- Captain of the Badminton Team and Libero of the Volleyball team in high school. Came 1st in 2018, 2nd in 2019 at the Inter-branch Badminton Tournament in college.
- Finished a full marathon (42 km) at Manipal Marathon 2020 with a timing of 6 hours and 33 minutes. [Certificate](#)
- Responsible for Field Work and Community Service activities in my high school for a week every term. Field Work involves planting saplings and shovelling while Community Service includes tidying up the school corridors and the school auditorium.

## LEADERSHIP

---

- Leader of a small group of Computer Vision enthusiasts within Research Society Manipal(RSM). Mentoring my juniors on Explainable AI and Interpretable ML projects.
- Mentor at OpenMined. I guide community members who are interested in Computer Vision to the field of XAI.