Yash Maurya

☎ 412-214-2983 ✉ ymaurya@cs.cmu.edu in yashmaurya yashmaurya01 yashmaurya.com

Objective

I am passionate about the convergence of Privacy, Machine Learning, Responsible and Explainable AI.
I hope to work on reliable and robust privacy designs for the societal good.

Education

Carnegie Mellon University, Pittsburgh **Aug 2023 – Dec 2024**
Master of Science in Information Technology - Privacy Engineering *GPA: 3.97/4*

Manipal Institute of Technology, Manipal **July 2018 – July 2022**
Bachelors of Technology in Computer and Communication Engineering *GPA: 8.49/10*

Experience

Carnegie Mellon University **Jan 2024 – Present**
Research Assistant *Pittsburgh, PA*

- Developing a user-focused Privacy and AI Threat Modeling framework funded by PwC's Digital Transformation and Innovation Center

Samsung Electronics **July 2022 – Aug 2023**
R&D Engineer *Noida, India*

- Submitted proposal for Samsung Discover 2.0 by adding new features using knowledge graphs & panoptic segmentation
- Collaborated with IIT-Delhi to engineer innovative taxonomy construction pipelines from raw data, enhancing robustness of Samsung News' new recommendation system

Samsung Electronics **Feb 2022 – June 2022**
R&D Intern *Noida, India*

- Researched deep reinforcement learning in video compression, producing a comprehensive literature survey
- Engineered scalable lightweight recommendation systems using deep learning tailored for mobile devices

DynamoFL (YC W22) **Feb 2021 – Aug 2021**
Federated Learning Researcher *Remote*

- Researched convergence optimization methods and communication efficient techniques for using Federated Learning with Differential Privacy for computer vision datasets
- Implemented secure server aggregation algorithms to replicate claimed accuracy real-world datasets

Publications

Is it worth storing historical gradients? | *Paper link* **Dec 2023**

- Empirically demonstrated that targeted adversarial attacks in Federated Learning can be effectively identified without historical gradients, enhancing privacy through data minimization and reinforced with differential privacy techniques.

Federated Learning for Colorectal Cancer Prediction | *Publication link* **June 2022**

- Developed a Federated Learning system for Colorectal Cancer Prediction, preserving client privacy while achieving an 86.2% accuracy, on par with the centralized model for IID clients

Improved variants of Score-CAM via Smoothing and Integrating | *Poster link* **June 2021**

- Improved Score-CAM by adding smoothing and integration functions as suggested in the SmoothGrad and IntegratedGrad papers.

IS-CAM: Integrated Score-CAM for axiomatic-based explanations | *Preprint link* **Oct 2020**

- Inspiration from integration in "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.

Certifications

Certified Information Privacy Technologist (CIPT) | *Credential* **Jan 2024**

- IAPP - International Association of Privacy Professionals

Projects

Space-JEDI (Junk Elimination and Debris Interception) | *Github link* **Sept 2023**

- Innovative system that predicts satellite trajectories and devises optimal **space debris** collection routes, leveraging real-time NASA data for effective orbital object management
- Space Theme Winner at HackCMU'2023 hackathon, built in under 20 hours