Yash Maurya

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

Education

Carnegie Mellon University — **Pittsburgh, PA**
Master of Science in Information Technology - Privacy Engineering - GPA: 3.97/4 — Aug 2023 – Dec 2024
- **Course Highlights:** Differential Privacy, Information Security, Federated Learning, Usable Privacy & Security, Policy, Law, Prompt Engineering, AI Governance

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

Experience

Carnegie Mellon University — **Pittsburgh, PA**
Independent Researcher (Advised by Virginia Smith) — Jan 2024 – Present
- Exploring Unlearning in LLMs

Research Assistant — Jan 2024 – Present
- Developing a user-centric notice and choice Privacy and AI Threat Modeling framework funded by PwC

Samsung Electronics — **Noida, India**
R&D Engineer — July 2022 – Aug 2023
- Built new features for Samsung Discover 2.0 using knowledge graphs & panoptic segmentation
- Engineered innovative taxonomy construction pipelines from raw data, enhancing robustness of Samsung News' new recommendation system in collaboration with IIT-Delhi

R&D Intern — Feb 2022 – June 2022
- 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) — **Remote**
Federated Learning Researcher — Feb 2021 – Aug 2021
- 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

Projects

Is it worth storing historical gradients? | *Github 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.

Digital Identity: A User-Centric Study | *Report link* — **Dec 2023**
- Highlights nuanced impact of Google's personalized advertising on user behaviors and perceptions.
- Reveals balance between digital identity, privacy, and engagement.

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

Certifications

Certified Information Privacy Technologist (CIPT) | *Credential* — **Jan 2024**
- IAPP - International Association of Privacy Professionals

Publications

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 (Accepted at IEEE GCAT'22)

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. (Accepted at Responsible Computer Vision Workshop at CVPR'21)

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.