Yash Maurya

412-214-2983 ymaurya@cs.cmu.edu 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

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
- Leveraged C++, Python, PyTorch, Keras and Android SDK to drive project success

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
- Applied Java, Python, Tensorflow.js, PyTorch, and Android to develop and deploy recommendation systems

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
- Conducted experiments in various data settings, including Vertical (SplitNN), Horizontal, and Hybrid FL
- Utilized PySyft, Flower, Opacus, PyTorch, Python, JavaScript, HTML, CSS, and AWS to accomplish project goals

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 Global Conference for Advancement in Technology '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 as an extended abstract at RCV 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.
- IS-CAM performs better than SS-CAM and Score-CAM in terms of faithfulness evaluations, considering the VGG-16 as our baseline model.

Projects

Space-JEDI (Junk Elimination and Debris Interception) | *Real-time Path Optimization, Web Dev* **Sept 2023**

- Innovative solution predicts satellite positions and plots optimal space garbage collector flight plans
- By continuously tracking and analyzing real-time data from NASA, JEDI is able to effectively monitor and manage objects in Earth's orbit
- Space Theme Winner at HackCMU'2023 hackathon, built in under 20 hours

Skills

Privacy and AI: Privacy Regulations Compliance, Differential Privacy, Data Anonymization, Secure Computing, Privacy-Enhancing Tools, Data Ethics, Secure Communication Protocols, Risk Assessment, Cybersecurity Awareness

Soft Skills: : Cross-functional Collaboration, Leadership, Project Management, Ethical Decision-Making