PRAHALADH CHANDRAHASAN

(412) 339 - 7156 | prahalac@andrew.cmu.edu | in/prahaladhchandrahasan

EDUCATION

CARNEGIE MELLON UNIVERSITY *Pittsburgh, PA*

Master's in Information Technology Privacy Engineering *Aug 2024-Dec 2025*

Relevant Coursework: Differential Privacy, Machine Learning, Advanced NLP, AI Governance, Deep Learning, Statistics

PROFESSIONAL EXPERIENCE

Research Assistant - LTI Carnegie Mellon University *Pittsburgh, PA*

Machine Learning Engineer *Jan 2025 - Present*

- Architected infrastructure to host benchmarking for RAG systems, enabling live comparison between various RAG systems
- Enhanced existing infrastructure to support multimodal RAG applications, incorporating image, text, and other data types
- Designed and implemented production-ready end-to-end RAG systems on AWS, from data ingestion to query processing
- Developed comprehensive evaluation pipelines using AWS Step Functions
- Built a custom RAG visualization tool by extending the ZenoML library.

Research Assistant - S3D CARNEGIE MELLON UNIVERSITY *Pittsburgh, PA*

Privacy Engineer *Jan 2025 - Present*

- Performed threat modelling for Privacy and Notice and Choices using a newly developed User's first framework
- Identified Various Privacy Notice and Choice threats for various contexts for an Online glass retailer application

Bank of America Continuum India *Chennai, India*

Software Engineer *Jul 2022-Jul 2024*

- Automated End-to-End payment flows from initiation to clearing for the bank's transformation to Real-Time Payment
- Developed Tosca UI and API modules that are reusable across multi-regional payment landscapes
- Identified Critical defects, saving the bank around 5 million dollars.
- Co-ordinated releases by testing production defect fixes across various environments
- Introduced various process automation through Tosca and Java saving the bank around 1000+ man hours
- Reviewed 10+ potential patentable ideas across the GCIBT sphere

RedHat *Bangalore, India*

Software Engineer Intern *Jan 2022-Jul 2022*

- Worked with the RedHat Fuse team, contributed to and maintained the Hawtio open-source project
- Pushed two features ENTESB-18633 and ENTESB-18785 in the latest release: 7.11
- Developed UI for the Hawtio project using AngularJS and Patternfly framework
- Introduced GitHub actions to the entire Hawtio project which automatically closes old issues

Dynamo FL (YC W22) *Chennai, India*

Federated Learning Intern *Oct 2021-Nov 2021*

- Implemented various Federated Learning algorithms from research papers using Pytorch
- Implemented differential privacy using the Pysyft library
- Designed and implemented experiments for testing out various hypotheses

RESEARCH PROJECTS

Gender Bias in LLMs

- Analyzed gender bias in LLMs through Big Five personality traits using statistical measures across multiple models.
- Developed metrics to quantify gender stereotype alignment and bias amplification in AI personality expressions.
- Extended PNAS research with robust experimental design testing 10 gendered prompts across various model architectures

Comparing Privacy guarantees of PPML libraries

- Trained CNN's with a given architecture for CIFAR-10 with Differential Privacy.
- Launched a Membership Inference Attack on DP-trained models using Shadow Models.
- Found a highly specific scenario where Opacus leaked more data than TF-Privacy.

Federated Learning for Colorectal Cancer Prediction

- Proposed a benchmark for using distributed training on the PathMNIST dataset.
- Evaluated both IID and Non IID dataset distributions up to 32 clients.
- Achieved comparable accuracy on IID settings with 32 clients tot the central model.

SKILLS

Languages and Frameworks: C, C++, Python, Java, SQL , Bash, JavaScript, , HCL, TensorFlow, Pytorch, GIT, Tricentis Tosca, Boto3, PySyft, Opacus, Rasa, Flask, TF Privacy , LangChain, HuggingFace, OpenAI, Kubernetes, Docker, AWS ECR, EKS, S3

Privacy Frameworks & Standards: LINDDUN, MITRE PANOPTIC, OWASP, Privacy-by-Design, NIST AI RMF, User's First