

Prahaladh Chandrahasan

412 339 7156 | prahalac@andrew.cmu.edu | [linkedin.com/prahaladhchandrahasan](https://www.linkedin.com/prahaladhchandrahasan)

Education

Carnegie Mellon University

Master's in Information Technology Privacy Engineering

Pittsburgh, PA
Aug 2024-Dec 2025

Relevant Coursework: (Differential Privacy, Machine Learning, Advanced NLP, AI Governance)

Research Areas:RAG Evaluation metrics, PETs(Privacy Enhancing Technologies), Privacy Preserving ML, Privacy Threat Modelling

Manipal Institute of Technology

Bachelor's in Information Technology

Manipal, India
Jul 2018-Jul 2024

Relevant Coursework: Data Structure and Algorithms, Operating Systems, Database Systems, Distributed Systems, Neural Networks

Experience

Bank of America Continuum India

Software Engineer

Chennai, India
Jul 2022-Jul 2024

- Automated End-to-End payment flows from initiation to clearing for the bank's transformation to Real-Time Payments.
- 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

Software Engineer Intern

Bangalore, India
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

Federated Learning Intern

Chennai, India
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

Cloudanix (YC S21)

Software Engineer Intern

Chennai, India
Mar 2021-Aug 2021

- Developed cloud compliance rules for **AWS** accounts using the **Boto3 Python SDK**
- Mapped service provider-specific conformity rules to the controls that specify security and governance requirements

Engineering Projects

Comparing Privacy guarantees of PPML libraries | Python, Opacus, TensorFlow-privacy, WandB

Sept 2024-Oct 2024

- 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 | Pytorch

Jan 2022-Jun 2022

- 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.

Crowd Scene Analysis | Python, Pytorch, Sci-kit learn,

Jan 2021-Jun 2021

- Proposed a robust and computationally efficient method for classifying a given crowd scene's HAD vectors.
- Performed hyperparameter tuning and K-Fold CrossValidation to find the top3 best performing classifiers.
- Quantized the angular deviation values into bins of various sizes to examine the effect of reducing the feature size.

Awards and Achievements

- Received the Arpit Jain Best Researcher Scholarship for FY-2022-23.
- Filed a patent on Payments Fraud detection within the first year of my professional journey.
- Bagged 2nd place (Across India) in BRICS Future Skills Aerial robotics organized by WorldSkills Russia.

Publications

- [Motion pattern-based crowd scene classification using histogram of angular deviations of trajectories](#). In The Visual Computer (2022).
- [Federated Learning for Colorectal Cancer Prediction](#), in 2022 IEEE 3rd Global Conference for Advancement in Technology (GCAT), 2022
- Distributed, Privacy-Preserving, Payments Fraud Detection System. **Application No.18/239,214**. [Patent]

Skills

Languages: Advanced: C, C++, Python | Intermediate: Java, SQL | Basic: Bash, JavaScript

Technologies: Advanced: TensorFlow, Pytorch, GIT, Tricentis Tosca, Boto3 | Intermediate: PySyft, Opacus, Rasa, Flask, TF Privacy,WandB, Fast_DP(AWS) , LangChain, HuggingFace, OpenAI,

Privacy Frameworks & Standards: NIST Privacy Framework, LINDDUN, MITRE PANOPTIC, FIPPs, OWASP, Privacy-by-Design, NIST AI RMF

Privacy Assessments & Documentation: Data Protection Impact Assessments(DPIAs), ROPAs, PIAs, Consent Management, Data Flow Mapping