SIKHA PENTYALA

+1(206) 724-4643 ◇ Seattle, WA ◇ sikha@uw.edu ◇ linkedin.com/in/sikhapentyala ◇ sikhapentyala.github.io/

EDUCATION

Ph.D. in Computer Science and Systems
University of Washington Tacoma — from Spring 2022

Master of Computer Science
University of Washington Tacoma (**GPA: 4.00**) — 2019 - 2020
Coursework: Data Structures and Algorithms, Distributed Systems, Machine Learning and Big Data Analytics

Post Graduate Diploma in Nuclear Engineering
Homi Bhabha National Institute (**GPA: 4.00**) — 2010 - 2011

Bachelor of Computer Science
Jawaharlal Nehru Technological University, Anantapur (**Gold Medalist - GPA: 4.00**) — 2005 - 2009

EXPERIENCE

Mila - Quebec AI Institute — Jul 2022 - Sep 2022
Research Intern — *Remote*

- Research on privacy preserving fair item rankings.

Mila - Quebec AI Institute — Oct 2021 - Mar 2022
Research Intern — *Remote*

- Research on training machine learning models in a federated environment while preserving privacy of the users and achieving group fairness.

University of Washington, Tacoma — Mar 2021 - Sep 2021
Research Assistant — *Tacoma, WA*

- Participation in IDASH Track III Challenge.
- Privacy-preserving fairness auditing.

University of Washington, Tacoma - Microsoft — Jul 2020 - Oct 2020
Graduate Research Student — *Tacoma, WA*

- Studied and designed system to automatically fix connectivity issues in existing Open Street Maps (OSM) dataset for its efficient use in routing services using C# in Visual Studio.
- System detected wrongly connected roadways to nodes for each country - 11% in New Zealand, 8% in the Fiji Islands, 19% in Venezuela and 8% in Serbia.

Nuclear Power Corporation of India Ltd. — Sep 2011 - Apr 2018
Scientific Officer — *Kudankulam, TN, India*

- Led a team of 2 developers to implement and re-design the intranet website to automate and achieve 50% faster process-lines, reducing labor and time costs.
- Estimated and managed cost, work scope, manpower, schedule and delivery for the intranet website while leading a team of 2 software developers.
- Designed business specific applications for website such as online tender preparation, a complaint management system, a works and contracts management system and a chemistry data management system.
- Increased up-time by 20% by moving 10 legacy systems to new hardware and software while administering 14 server hardware as well as 27 software applications.

RELEVANT PUBLICATIONS

- **S. Pentyala**, R. Dowsley and M. De Cock *Privacy-Preserving Video Classification with Convolutional Neural Networks*, 38th International Conference on Machine Learning, PMLR 139, 2021.
- **S. Pentyala**, M. De Cock and R. Dowsley *Privacy-Preserving Video Classification*, WiCV 2021 *(poster in Women in Computer Vision Workshop at CVPR, 2021)*

- **S. Pentyala**, D. Melanson, M. De Cock and G. Farnadi *PrivFair: a Library for Privacy-Preserving Fairness Auditing*, PPAI-2022 *(AAAI-22 Workshop on Privacy-Preserving Artificial Intelligence (8 pages))*
- **S. Pentyala**, et al. *PrivFairFL: Privacy-Preserving Group Fairness in Federated Learning*, MAIS 2022
- **S. Pentyala**, et al. Towards private and fair federated learning WiML@NeurIPS 2022
- **S. Pentyala**, et al. *Training Differentially Private Models with Secure Multiparty Computation*, *(Under Review)*

AWARDS

- WiML travel funding award (WiML@NeurIPS 2022)
- Carwein-Andrews Endowment award for 2022-2023, UW Tacoma, School of Engineering and Technology
- 2021-2022 School of Engineering Technology's Outstanding Graduate Research Award, UW Tacoma
- Winner of Track III of the iDASH2021 secure genome analysis competition
- Gold Medalist at Jawaharlal Nehru Technological University, Anantapur in the Branch of ECM, Class of 2009

SKILLS

Programming Languages	Java, Python, C#
Frameworks	MP-SPDZ, FairLearn, Flower, PySyft
Tools and Technologies	Keras, Sklearn, Pandas, TensorFlow, Pytorch, OpenCV, Docker, Git (Github), Jupyter
Databases	DynamoDB, MS-SQL, ORACLE DB, MySQL
Cloud Technologies	Amazon Web Services (AWS - EC2, S3), Azure
Servers	Apache-Tomcat, WAMP/LAMP, MS AD-DC and Exchange, BlueCoat

RELEVANT PROJECTS

Privately classifying a video using Convolutional Neural Networks - MPC.

- Built first end-to-end secure multi party computation protocol (MPC) for private video classification in Python using MP-SPDZ benchmarking software and Tensorflow.
- Designed and trained a CNN with 1.5 million paramters to detect 7 emotions in a video from RAVDESS dataset.
- Deployed solution in cloud (AWS, Azure) & classified 4s video in 8.5s (passive 3PC) by keeping content of video and model parameters private to the owners in different adversarial models.

Privacy preserving fairness auditing - MPC and Fairness.

- Built first MPC protocols to compute statistical notions of group fairness such as equalized odds, demographic parity and subgroup accuracy for multi-class and binary classification in MP-SPDZ.
- Developed and deployed a demo web-based service that takes images or tabular data from one user and model parameters from the other user and performs secure auditing of the model using above MPC protocols. Audited a CNN with 1.48 parameters with 56 images in 30 secs in a 3PC passive setting.

Confidential Computing - Federated learning, MPC and Differential privacy.

- Built a solution where two parties individually train a DP logistic regression (LR) model and obtain aggregated ϵ-DP LR model. Achieved a test accuracy of 85.79% with the model trained in 0.27s in the competition.
- Built a solution where multiple parties collaborate to train a DP LR model using MPC, suitable for multiple scenarios of data splits. Achieved a test accuracy of 87.98% in 76s in a 3PC passive setting.

Private and Fair ML training - Federated learning, Privacy and Fairness.

- Devise techniques to achieve group fairness in the federated learning while preserving privacy of the users and their sensitive attributes.
- Developed MPC protocols for existing central pre-processing and post-processing techniques to adapt in a FL setup in privacy-preserving way.
- Evaluated proposed techniques using Flower framework with 100+ clients.

Recommendation system - Privacy and Fairness.

- Devised techniques to preserve consumer (users) privacy while achieving fairness for producers (items).

Private Financial Crime Detection - Privacy

- Ongoing Project on designing privacy-preserving Federated learning solution to train models to detect anomalies in financial transactions.