SIKHA PENTYALA

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

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 — Oct 2021 - Mar 2022
Research Intern — *Remote*

- Research on training recommendation system 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*

- Research on fairness in machine learning (using FairLearn) by participating in RecSys 2021 Challenge.
- 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.
- 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.
- Developed an application for exploring and fixing connectivity errors in OSM using C# in Visual Studio.

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.
- Revamped frontend existing intranet website using HTML and JavaScript while implementing business logic using JAVA with queries in MS-SQL.
- 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.
- Improved Annual Budget Exercises(Capital & Revenue) thru' web application leading to 70% faster delivery of budget and cost reports for each department and completion of discussion rounds for adhoc cuts.
- Performed market survey and procurement activities for IT infrastructure to purchase products at best offered price.

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.

- F. Tabet and **S. Pentyala**, B. Patel, et al. *OSMRunner: A System for Exploring and Fixing OSM Connectivity*, 22nd IEEE International Conference on Mobile Data Management (MDM) 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. *Training Differentially Private Models with Secure Multiparty Computation*, *(Under Review)*
- **S. Pentyala**, et al. PrivFairFL: Privacy-Preserving Group Fairness in Federated Learning, *(Under Review)*

AWARDS

- 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

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 for statistical notions of group fairness such as equalized odds, demographic parity and subgroup accuracy for multi-class and binary classification in MP-SPDZ.
- Built MPC protocols for image classification using a CNN and text classification using a logistic regression.
- Analyzed performance of the MPC protocols for 2PC and 3PC in passive and active security settings for text and image classification. Audited a CNN with 1.48 parameters with 56 images in 30 secs in a 3PC passive setting.
- Developed and deployed a demo web-based service that takes images or text form one user and model parameters from the other user and performs secure auditing of the model using above MPC protocols.

Confidential Computing - Federated learning, MPC and Differential privacy

- Built a solution where two parties individually train a logistic regression (LR) model, add Laplacian noise and publish the differentially private (DP) models. The published model parameters are aggregated by each party resulting in a final ϵ-DP LR model trained in a federated environment.
- Achieved a test accuracy of 84.85% with the model trained in 0.27s in the competition.
- Added regularization for the LR training module in MP-SPDZ library. Collaborated to train a LR model using MPC (2PC-passive).
- Collaborated in implementing MPC protocol to add a noise vector to the secret-shared model coefficients of the LR model, after which the resulting shares are disclosed so that they can be combined to get a final ϵ-DP LR model.

Recommendation system - Federated learning, Privacy and Fairness

- Training a logistic regression in a federated learning environment using Flower framework.
- Experimenting with techniques to achieve group fairness for users based on sensitive attributes such as gender, income and age.
- Devise techniques to achieve group fairness in the federated learning while preserving privacy of the users and their sensitive attributes.
- Developing MPC protocols for existing central pre-processing and post-processing techniques to adopt in a FL setup in privacy-preserving way.