+1 (608)640-2965
csarthak76@gmail.com
linkedin.com/in/sarthak-choudhary
google.scholar/sarthak-choudhary

SARTHAK CHOUDHARY

EDUCATION

2024 **University of Wisconsin-Madison**
Ph.D. in Computer Science (2024 - Present)

2019 **Birla Institute of Technology and Science, Pilani** CGPA: **8.78/10.0**
Bachelors of Engineering (Hons) in Computer Science (2019 - 23)

TECHNICAL SKILLS

Languages: C, C++, Python, R, Golang, Solidity
FrameWorks: Flower, FederatedScope, Brownie, Django, Flask, Apollo, Express
Technologies: PyTorch, PyTorch Distributed, Docker, AWS, DigitalOcean, Chainlink, gRPC, Elasticsearch, GDAL

ACADEMIC POSITIONS

2022 **Teaching Assistant** for CS-F211 (Data Structures and Algorithms)

2021 **Teaching Assistant** for CS-F214 (Logic in Computer Science)

ACADEMIC ACHIEVEMENTS

2021 Selected for **Mitacs Globalink Research Internship** under **Prof. Sergio Rossi**, Université du Québec à Chicoutimi - Chicoutimi

PUBLICATIONS

2024 **Attacking Byzantine Robust Aggregation in High Dimensions** - **Choudhary, S.***, Kolluri, A.* and Saxena, P.

2023 **Scalable Neural Network Training over Distributed Graphs** - Kolluri, A.*, **Choudhary, S.***, Hooi, B. and Saxena, P.

2023 **Pub-SubMCS: Privacy-Preserving Publish-Subscribe based Decentralized Framework for Mobile Crowdsensing.** - Agrawal, A., **Choudhary, S.**, Bhatia, A. and Tiwari, K.

EXPERIENCE

Visiting Scholar | Security Research Lab, National University of Singapore Aug 2022 - July 2024

Mentor: Prof. Prateek Saxena, Associate Professor, NUS School of Computing

- Conducted in-depth research on **Byzantine Robust Aggregation** in High Dimensions, culminating in the development of a groundbreaking attack named HIDRA, disrupting state-of-the-art defenses.
- Studied state-of-the-art **Graph Neural Networks** and implemented a novel framework GLIDE for scalable neural network training over distributed graphs with minimal communication cost.
- Studied the latest **Robust Mean Estimation** algorithms for high dimensional inputs addressing their computational complexity.
- Studied **Continuous Verifiable Delay Functions** and the interactive proof for the hardness assumption of Verifiable Delay Functions as course exercise of *CS6321 Advanced Topics in Security and Privacy* at NUS.

*equal contrbution

Software Development Intern | The D. E. Shaw Group, India May 2022 - July 2022

Mentor: Mudit Dangi , Project Lead, The D. E. Shaw Group

- Developed an **Elasticsearch** service to detect duplicate applicants using full text search using **Java API Client** and **QueryBuilder**.
- Migrated the existing codebase to **Command Pattern** design in Java.
- Implemented grouping algorithm for duplicate matches to resolve the matches in a responsive setup.
- Devised an algorithm to calculate similarity score considering attributes from the applicant's resume.

Research Intern | North Eastern Space Application Centre, Umiam May 2021 - July 2021

Mentor: Nilay Nishant, Scientist/Engineer-SD, NESAC

- Implemented a python package to perform interactive remote sensing operations in python shell.
- Developed a **Django** server to support remote sensing queries from the package.
- Developed endpoints to fetch satellite images (raster data) using **GDAL** to get **RGBA** expansion of the images and to calculate built-up area using ML models.
- Integrated the python package with **ipyleaflet** to render raster data using python shell.

PROJECTS

Byzantine Robust Gradient Aggregation

Research Project, Prof. Prateek Saxena, National University of Singapore | Paper | Code

- Assessed the susceptibility of robust high-dimensional input aggregation by analyzing state-of-the-art aggregators in the face of adversarial corruptions.
- Emphasized the computational complexity of the most recent defenses, highlighting its impact on the optimal guarantees offered by them when implemented in a practical setup.
- Pioneered the first successful attack against state-of-the-art robust gradient aggregation algorithms such as **Filtering**, **No-Regret**, and **GAN**, through the exploitation of their computational bottlenecks.
- Investigated the attack's impact on CNN training procedures, revealing a substantial accuracy drop of up to **80**% across major benchmark datasets, including **MNIST**, **Fashion-MNIST**, and **CIFAR10**.

Retexo

Research Project, Prof. Prateek Saxena, National University of Singapore | Paper | Code

- Implemented a novel framework GLIDE for scalable neural networks training over distributed graphs.
- Used the framework with state-of-the-art GNNs such as **GCN**, **GraphSAGE**, and **GAT** to conduct supervised node classification on distributed graphs, achieving a remarkable **30**× improvement in communication efficiency.
- Assessed task accuracy and communication efficiency in an end-to-end setup, distributing popular graph datasets across multiple Raspberry Pis using the '**Flower**' federated learning framework.

Pub-SubMCS

Research Project, Prof. Ashutosh Bhatia, BITS Pilani | Paper | Code

- Developed an innovative blockchain-based distributed crowdsensing framework utilizing a publish/subscribe architecture.
- Implemented the framework using **Solidity** with the Brownie development tool and deployed the contracts on the **Kovan** test network.
- Utilized **Chainlink** Keepers to create time-based triggers for contract functions.
- Addressed the limitations of the Requester-Worker model in crowdsensing by optimizing efficiency through the grouping of multiple requesters to minimize redundancy.