Barath Kumar GaneshKumar

beekayg15.github.io | Brooklyn, NY, USA | +1 (347) 236-9492

Education

New York University, Courant — NYC, USA
M.S. in Computer Science; GPA: 3.95/4.00 — September 2023 - May 2025

PSG College of Technology — Coimbatore, India
B.E. in Computer Science and Engineering; CGPA: 9.86/10.00 — July 2019 - May 2023

Research Interests

- Doubly-Efficient Interactive Proofs
- Zero-Knowledge Proofs
- Foundations of Cryptography
- Complexity Theory
- Spectral Graph Algorithms

Research Experience

Accumulation without Homomorphism with Dr. Benedikt Bünz — Fall 2024

- Developing the accumulation scheme without homomorphic commitments as suggested in [BMNW24] using quantum-secure Merkle trees and error correcting codes using Arkworks
- Reviewing relevant literature to develop and optimize the Accumulation scheme

Doubly-Efficient Interactive Proofs with Dr. Marshall Ball — Fall 2024

- Studying the Doubly-Efficient Interactive Proof systems proposed earlier in [GRK], [RRR], and [GR], and researching on existence of classes beyond $\mathcal{NC}$ and $\mathcal{SC}$ for which doubly-efficient proof systems exist

Improving Generalized Cheeger's Inequality with Dr. Anupam Gupta — Fall 2024

- Studying the possibility of improving the upper bound of the generalized k-order Cheeger's Inequality

Implementing Zero Cash Sapling Protocol with Dr. Benedikt Bünz — Spring 2024

- Partnered with a fellow student to implement the ZCash Sapling protocol as a part of *CSCI-GA.3033 Cryptography of Blockchains*
- Utilized Arkworks, a Rust-based library for zk-SNARKs, to implement the Spend and Output circuits of the Zero Cash framework
- Optimized the framework by reducing the number of constraints by approximately 40,000 through the integration of the Poseidon hash function, replacing the previously used Blake hash

Defense Against Evasion Attacks in ML Models with Dr. Sudha Sadasivam — Spring 2023

- Simulated evasion attacks on image classification models, under various assumptions on the amount of prior knowledge known to the attackers, about the system
- Analysed the effectiveness and efficiency of the evasion attacks on the classifier and its impact on the performance of the model in terms of the confidence score, precision, robustness and F1-score
- Proposed a defense mechanism involving retraining of the model repeatedly, adjusting the weights, to classify even the adversarial examples of the evasion attack, correctly

Privacy Preserved and Secure Federated Learning with Dr. Sudha Sadasivam — Fall 2022

- Developed a Federated Learning model, to overcome the security related shortcomings of the standard machine learning models, for recognizing patients suffering from dyslexia
- Incorporated privacy-preserving mechanisms such as Differential Privacy, Homomorphic Encryption, and Secure MultiParty Computation into the federated learning model
- Analyzed the accuracy achieved by the developed model against different levels of privacy, by fine-tuning the amount of Laplacian and Gaussian noise introduced to the gradients

Unified Parsing Script using Machine Learning with Dr. Sudha Sadasivam Spring 2022

- Worked on overcoming the issues associated with the primitive web scrapers such as being site-dependent and highly rigid to changes in the HTML template
- Used three independent machine learning models that recognize patterns in the position of the desired information in the website, it's dimensions and the HTML tag enclosing it respectively
- By embedding the three models together, developed a site independent machine learning system, that extracts key information from different web pages from a variety of e-retailer sites
- Achieved an accuracy of 96% in extracting the key information from previously seen sites and an accuracy of 82% in extracting information from previously unseen web sites

Offload Decision Making for Web Applications with Dr. Sudha Sadasivam Fall 2021

- Conceived a novel machine learning model that makes decisions to execute JavaScript compute units locally or remotely by predicting and comparing the time of execution in the local machine and 7 different servers by analyzing execution time of 10000+ executions of similar complexity algorithms in each server
- Achieved an accuracy of 87.1% in predicting the execution time of a given application in multiple devices using a single model and an accuracy of 89.2% in making the correct offloading decision and reduced the average time to execute a compute unit by 37%

Work Experience

Amazon Development Center Chennai, India
Software Development Engineer Intern January 2023 - June 2023

- Worked in Full-Stack Development as a part of the 6-member SQS-CTT under the Digital Support Engineering Division.
- Investigated and implemented an efficient technique to record page-level metrics across 3 applications at minimum cost, saving 5 hours per week of manual analysis.
- Enhanced the processing and visualizing of 30+ web vitals, 500+ frequently occurring errors, and navigation trends of 12000+ active users, using AWS CloudWatch RUM
- Developed 'Insights and Conversations' feature for 1100 internal testers and 200+ stakeholders to raise concerns and record insights on 13 testing metrics and start interactive conversations on the insights.

Samsung R&D Institute India Bangalore, India
Project Intern May 2021 - November 2021

- Worked alongside the IoT team as a part of the Samsung PRISM program.
- Experimented and developed machine learning models to solve the *Offload Decision Making* problem under the guidance of Mr. Suyambulingam Rathinasamy Muthupandi
- Received a 'Certificate of Excellence' for the work done in solving the assigned problem

Relevant Coursework

Geometric Methods for Algorithm Design, Fundamental Algorithms, Cryptography of Blockchains Introduction to Graduate Cryptography, Operating Systems, Programming Languages, Social and Economic Network Analysis, Deep Learning, Machine Learning, Advanced Data Structures, Undergraduate Cryptography, Artificial Intelligence, Distributed Systems

Teaching Experience

NYU CSCI-GA.2250-001 Operating Systems, *Grading Assistant* Fall 2024
NYU CSCI-UA.0480-063 Introduction to Computer Security, *Grading Assistant* Fall 2024

Awards

Best Outgoing Student, Batch of 2023, *PSG College of Technology* May 2023
Gold Medalist, Batch of 2023, *PSG College of Technology* July 2023

Publications

[with G. Sudha Sadasivam, R. Tarun Visva, S. Mukesh, R. Shashaank, Preeti Muley]
Unified Parsing Script using Machine Learning, International Conference on Artificial Intelligence and Signal Processing (AISP), 2023.

[with G. Sudha Sadasivam, R. Tarun Visva, B. Hrithik, M. Aravind, A. Bhooshaan]
Offload Decision Making for Web Applications, International Conference on Intelligent Systems for Communication, IoT and Security (ICISCoIS), 2023

Presentations

Unified Parsing Script using Machine Learning, School of Electronics Engineering, VIT-AP University, Amaravati. (March 2023)

Offload Decision Making for Web Applications, Department of Information Technology, PSG College of Technology, Coimbatore. (February 2023)

Community Involvement

NYU Theory Seminar, 2023 - 2025
NYU Crypto Seminar, 2024 - 2025
Secretary, Computer Science and Engineering Association, PSGCT, 2022 - 2023
Joint Secretary, Computer Science and Engineering Association, PSGCT, 2021 - 2022
Problem Setter, Coding Club, PSGCT, 2021 - 2022

References

Dr. Marshall Ball
Assistant Professor of Computer Science at NYU Courant

Dr. Benedikt Bünz
Assistant Professor of Computer Science at NYU Courant

Dr. Anupam Gupta
Professor of Computer Science at NYU Courant

Dr. Sudha Sadasivam
Head of the Department, Department of Computer Science, PSGCT