Bargav Jayaraman

bj4nq@virginia.edu | https://bargavjayaraman.github.io

Education

PhD in Computer Science (May ’22)
University of Virginia, Charlottesville, USA
GPA: 3.91/4.0

MS in Computer Science (May ’15)
IIIT, Hyderabad, India
GPA: 8.68/10.0

B Tech in Computer Science (May ’12)
SASTRA University, Thanjavur, India
GPA: 8.58/10.0

Technical Skills

Languages:
Python, C, C++, Java

Web Development:
HTML, CSS, Markdown

Libraries & Frameworks:
Scikit-Learn, Obliv-C, Tensorflow, Amazon Web Services, Git

Work Experience

Research and Development Senior Analyst

Jan ’15 to July ‘16

Accenture Technology Labs, Bangalore, India

- Application of machine learning techniques for solving software engineering problems like multi-lingual vagueness detection on software requirements and automated web testing.
- Filed *three* patents and co-authored a peer-reviewed paper accepted in 25th conference on RE ’17.
- Developed end-to-end deep learning pipeline for detecting vagueness in English and transferring the vagueness detection knowledge to Portuguese and Spanish.
- Used deep learning techniques to identify web objects and texts for automated testing of web pages.

Teaching Assistant for following courses:

- Data Warehousing and Data Mining (at IIIT Hyderabad, India) *Fall ’14*
- Principles of Information Security (at IIIT Hyderabad, India) *Spring ’14*

Selected Projects and Publications

Evaluating Differentially Private Machine Learning in Practice

Aug ’18 to Present

- Compared the privacy leakage of differential private machine learning implementations.
- Proposed stronger membership inference attacks that pose significant privacy threat even in skewed prior settings.
- Implemented using Python and Tensorflow framework.

Related Publications: *In PETS ‘21* *In USENIX Security ‘19*

Private Multi-Party Machine Learning

Aug ’16 to Present

- Performed privacy preserving machine learning over sensitive data such as health records.
- Combined secure multi-party computation protocols with differential privacy to improve privacy-utility trade-off.
- Implemented using Python, Scikit-Learn and Obliv-C framework.

Related Publications: *In NIPS ‘18* *In NIPS ’16*

Distributed Certificate Authorities

Apr ’17 to July ‘17

- Proposed decentralized CA where two CAs jointly generate certificates using secure multi-party computation.
- Experimented with different bandwidth and latency settings on AWS and Azure cloud servers.
- Secure certificate signing in *minutes*, costing from *cents* to *few dollars*.
- Implemented certificate signing using Obliv-C and GMP libraries.

Related Publications: *In Archive ’17*

Multi-Lingual Vagueness Detection

Jan ’15 to Jan ‘16

- Used deep learning to identify vague terms like ‘some’, ‘many’, etc. in software requirement texts.
- Used transfer learning for vagueness detection across English, Spanish and Portuguese software requirements.
- Implemented using Theano and Python framework.

Related Publications: *In RE ’17*

Secure String Matching on Outsourced Data

Jan ’14 to Dec ‘14

- Performed searching of sub-strings and prefixes within keywords on documents outsourced to cloud server.
- Ranked documents containing the target string pattern in an efficient and privacy preserving way.
- Implemented in C++.

Related Publications: *In ICDCS ’15*