

CURRICULUM VITAE

Bargav Jayaraman

PhD Student in Computer Science
University of Virginia
330 Rice Hall, Charlottesville VA 22903

Email: bargavj@virginia.edu
Web: <http://bargavjayaraman.github.io/>

(a) Education & Training

University of Virginia	Charlottesville VA, USA	Computer Science	PhD, 2016 – present
IIIT Hyderabad	Telangana, India	Computer Science	MS, 2012 – 2015
SASTRA University	Tamil Nadu, India	Computer Science	B. Tech, 2008 – 2012

(b) Research & Professional Experience

2016 – present Graduate Research Assistant, University of Virginia
2015 – 2016 R & D Senior Analyst, Accenture Technology Labs Bangalore
Fall 2014 Teaching Assistant (Data Warehousing and Data Mining), IIIT Hyderabad
Spring 2014 Teaching Assistant (Principles of Information Security), IIIT Hyderabad

(c) Publications

On Privacy-Preserving Machine Learning

1. Bargav Jayaraman, Lingxiao Wang, Katherine Knipmeyer, Quanquan Gu, and David Evans. Revisiting membership inference under realistic assumptions. *arXiv:2005.10881*, 2020.
2. Lingxiao Wang, Bargav Jayaraman, David Evans, and Quanquan Gu. Efficient privacy-preserving stochastic nonconvex optimization. *arXiv:1910.13659*, 2020.
3. Bargav Jayaraman and David Evans. Evaluating differentially private machine learning in practice. In *USENIX Security Symposium*, 2019.
4. Bargav Jayaraman, Lingxiao Wang, David Evans, and Quanquan Gu. Distributed learning without distress: Privacy-preserving empirical risk minimization. In *Advances in Neural Information Processing Systems*, 2018.
5. Lu Tian, Bargav Jayaraman, Quanquan Gu, and David Evans. Aggregating private sparse learning models using multi-party computation. In *NeurIPS Workshop on Private Multi-Party Machine Learning*, 2016.

Other Publications

6. Bargav Jayaraman, Hannah Li, and David Evans. Decentralized certificate authorities. *arXiv:1706.03370*, 2017.
7. Breno D. Cruz, Bargav Jayaraman, Anurag Dwarakanath, and Collin McMillan. Detecting vague words and phrases in requirements documents in a multilingual environment. In *IEEE International Requirements Engineering Conference (RE)*, 2017.
8. Bruhadeshwar Bezawada, Alex X. Liu, Bargav Jayaraman, Ann L. Wang, and R. Li. Privacy preserving string matching for cloud computing. In *IEEE International Conference on Distributed Computing Systems*, 2015.

(d) Invited Talks and Presentations

1. Presented a poster on “Revisiting Membership Inference Under Realistic Assumptions” at *TPDP* and *PPML workshops* co-located with *CCS 2020* and *NeurIPS 2020* conferences resp.

2. Gave an invited talk at Microsoft Research in Summer 2020 where I presented my work on membership inference attacks on machine learning models.
3. Gave a talk on evaluating privacy-utility trade-off of privacy preserving machine learning at *AIML seminar* held at University of Virginia in Fall 2019.
4. Gave a talk on evaluating privacy preserving-machine learning at Winter 2019 *DCAPS workshop* held at University of Maryland College Park.
5. Presented my published work on “Evaluating Differentially Private Machine Learning in Practice” at *USENIX Security Symposium*, 2019.
6. Presented my published work on “Distributed Learning without Distress: Privacy-Preserving Empirical Risk Minimization” at *NeurIPS conference*, 2018.
7. Presented my published work on “Aggregating Private Sparse Learning Models using Multi-Party Computation” at *PPML workshop* co-located with *NeurIPS conference*, 2016.

(e) Awards and Achievements

1. Awarded travel grant at *USENIX Security Symposium*, 2019.
2. Awarded travel grant at *NeurIPS conference*, 2018.
3. Filed *three* patents while working at Accenture Technology Labs Bangalore.