CURRICULUM VITAE

Bargav Jayaraman
PhD Student in Computer Science
University of Virginia
330 Rice Hall, Charlottesville VA 22903
Email: bargavjayaraman@gmail.com
Web: http://bargavjayaraman.github.io/

(a) Education & Training

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

(b) Research & Professional Experience

Summer 2021	Research Intern, Microsoft Redmond Lab
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) Skill Set

Programming	Python, C, C++, Java
Frameworks	Scikit-Learn, PyTorch, Tensorflow, Obliv-C, AWS, Azure, Git
Web	HTML, CSS, Markdown

(d) Publications

Attacks On Machine Learning

1. Bargav Jayaraman and David Evans. Are attribute inference attacks just imputation? Manuscript submitted for publication, 2022.
2. Bargav Jayaraman, Lingxiao Wang, Katherine Knipmeyer, Quanquan Gu, and David Evans. Revisiting membership inference under realistic assumptions. In *Proceedings on Privacy Enhancing Technologies*, 2021.
3. Bargav Jayaraman and David Evans. Evaluating differentially private machine learning in practice. In *USENIX Security Symposium*, 2019.

Privacy-Preserving Machine Learning

4. Lingxiao Wang, Bargav Jayaraman, David Evans, and Quanquan Gu. Efficient privacy-preserving stochastic nonconvex optimization. *arXiv:1910.13659*, 2020.
5. 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.
6. 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

7. Bargav Jayaraman, Hannah Li, and David Evans. Decentralized certificate authorities. *arXiv:1706.03370*, 2017.
8. 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.
9. 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.

(e) Invited Talks and Presentations

1. Presented my published work on "Revisiting Membership Inference Under Realistic Assumptions" at *PETS Symposium*, 2021.
2. 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.
3. Gave an invited talk at Microsoft Research in Summer 2020 where I presented my work on membership inference attacks on machine learning models.
4. 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.
5. Gave a talk on evaluating privacy preserving-machine learning at Winter 2019 *DCAPS workshop* held at University of Maryland College Park.
6. Presented my published work on "Evaluating Differentially Private Machine Learning in Practice" at *USENIX Security Symposium*, 2019.
7. Presented my published work on "Distributed Learning without Distress: Privacy-Preserving Empirical Risk Minimization" at *NeurIPS conference*, 2018.
8. Presented my published work on "Aggregating Private Sparse Learning Models using Multi-Party Computation" at *PPML workshop* co-located with *NeurIPS conference*, 2016.

(f) 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.

(g) Professional Services

1. Program Committee Member for Privacy Preserving Machine Learning Workshop 2021
2. Program Committee Member for Privacy in Machine Learning Workshop 2021
3. Reviewer for ACM Conference on Computer and Communications Security Poster 2021
4. Reviewer for IEEE Transactions on Dependable and Secure Computing 2021