

## CURRICULUM VITAE

### Bargav Jayaraman

PhD, Computer Science

Research Scientist, Oracle Labs

35 Network Dr, Burlington MA 01803

Email: [bargavjayaraman@gmail.com](mailto:bargavjayaraman@gmail.com)

Web: <http://bargavjayaraman.github.io/>

#### (a) Research Interests

Privacy preserving machine learning, differential privacy, evaluation metrics for privacy leakage quantification, memorization in LLMs and VLMs, security and access control, federated learning.

#### (b) Education & Training

2016 – 2022	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

#### (c) Research & Professional Experience

Nov 2024 – Now	Research Scientist, Oracle Labs, Burlington
Jan 2023 – Nov 2024	Postdoctoral Researcher, Meta FAIR, Menlo Park
May 2021 – Aug 2021	Research Intern, Microsoft Research, Seattle
Aug 2016 – Dec 2022	Graduate Research Assistant, University of Virginia, Charlottesville
Jan 2015 – Jun 2016	R & D Senior Analyst, Accenture Technology Labs, Bangalore
Fall 2014	Teaching Assistant (DWD), IIIT Hyderabad, Hyderabad
Spring 2014	Teaching Assistant (POIS), IIIT Hyderabad, Hyderabad

#### (d) Skill Set

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

#### (e) Publications

##### *Attacks On Machine Learning*

1. Tom Sander\*, Bargav Jayaraman\*, Mark Ibrahim, Chuan Guo, and Kamalika Chaudhuri. Rethinking the Role of Verbatim Memorization in LLM Privacy. In *Advances in Neural Information Processing Systems*, 2025.
2. Narine Kokhlikyan\*, Bargav Jayaraman\*, Florian Bordes, Chuan Guo, and Kamalika Chaudhuri. Measuring Déjà Vu Memorization Efficiently. In *Advances in Neural Information Processing Systems*, 2024.
3. Bargav Jayaraman, Chuan Guo, and Kamalika Chaudhuri. Déjà Vu Memorization in Vision-Language Models. In *Advances in Neural Information Processing Systems*, 2024.
4. Bargav Jayaraman, Esha Ghosh, Melissa Chase, Sambuddha Roy, Wei Dai, and David Evans. Combing for Credentials: Active Pattern Extraction from Smart Reply. In *IEEE Symposium on Security and Privacy*, 2024.
5. Bargav Jayaraman and David Evans. Are Attribute Inference Attacks Just Imputation? In *ACM Conference on Computer and Communications Security*, 2022.
6. Bargav Jayaraman, Lingxiao Wang, Katherine Knipmeyer, Quanquan Gu, and David Evans.

Revisiting Membership Inference Under Realistic Assumptions. In *Proceedings on Privacy Enhancing Technologies*, 2021.

7. Bargav Jayaraman and David Evans. Evaluating Differentially Private Machine Learning in Practice. In *USENIX Security Symposium*, 2019.

### ***Security / Privacy / Access Control for Machine Learning***

8. Bargav Jayaraman, Virendra J. Marathe, Hamid Mozaffari, William F. Shen, and Krishnaram Kenthapadi. Permissioned LLMs: Enforcing Access Control in Large Language Models. In *Advances in Neural Information Processing Systems*, 2025.
9. Lingxiao Wang, Bargav Jayaraman, David Evans, and Quanquan Gu. Efficient Privacy-Preserving Stochastic Nonconvex Optimization. In *Uncertainty in Artificial Intelligence*, 2023.
10. 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.
11. 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***

12. Bargav Jayaraman\*, Hannah Li\*, and David Evans. Decentralized Certificate Authorities. *arXiv:1706.03370*, 2017.
13. 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.
14. 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.

### **(f) Invited Talks and Presentations**

1. Presented my published work on “Combing for Credentials: Active Pattern Extraction from Smart Reply” at *IEEE S & P*, 2024.
2. Presented my published work on “Are Attribute Inference Attacks Just Imputation?” at *ACM CCS*, 2022.
3. Presented my published work on “Revisiting Membership Inference Under Realistic Assumptions” at *PETS Symposium*, 2021.
4. 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.
5. Gave an invited talk at Microsoft Research in Summer 2020 where I presented my work on membership inference attacks on machine learning models.
6. 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.
7. Gave a talk on evaluating privacy preserving-machine learning at Winter 2019 *DCAPS workshop* held at University of Maryland College Park.

8. Presented my published work on “Evaluating Differentially Private Machine Learning in Practice” at *USENIX Security Symposium*, 2019.
9. Presented my published work on “Distributed Learning without Distress: Privacy-Preserving Empirical Risk Minimization” at *NeurIPS conference*, 2018.
10. Presented my published work on “Aggregating Private Sparse Learning Models using Multi-Party Computation” at *PPML workshop* co-located with *NeurIPS conference*, 2016.

**(g) 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.

**(h) Professional Services**

1. Program Committee Member: SatML - [2026, 2025], ICML - [2025, 2024], NeurIPS - [2025, 2024, 2023], USENIX Security 2023, PPML Workshop 2021 and Privacy in ML Workshop 2021.
2. Reviewer for ACM CCS 2021 and IEEE TDSC 2021.