Abhishek Singh

Ph.D. Student, MIT Media Lab
Massachusetts Institute of Technology

Education

2021–Present **Ph.D. student** *Camera Culture Group*, Advised by Prof. Ramesh Raskar

Current Research: Privacy, Distributed Machine Learning, Differential Privacy, Computer Vision.

2019–21 **MS, Research Assistant** *Camera Culture Group*, Advised by Prof. Ramesh Raskar

Current Research: Privacy preserving Machine Learning, Distributed machine learning, Digital Health, Computer Vision. Applied Cryptography.

Selected Papers (Please see Google Scholar for the full list)

NeurIPS(W) 2022 Frederic Berdoz, **Abhishek Singh**, Martin Jaggi, Ramesh Raskar. "*Scalable Collaborative Learning via Representation Sharing.*" Workshop on Decentralized and Trustworthy ML in Web3. (**Oral**)

ECCV 2022 **Abhishek Singh**, Ethan Garza, Ayush Chopra, Praneeth Vepakomma, Vivek Sharma, Ramesh Raskar. "*Decouple-and-Sample: Protecting sensitive information in task agnostic data release.*" European Conference on Computer Vision, 2022.

ECCV 2022 Ayush Chopra, Abhinav Java, **Abhishek Singh**, Vivek Sharma, Ramesh Raskar. "*Learning to Censor by Noisy Sampling.*" European Conference on Computer Vision, 2022.

ICML(W) 2022 **Abhishek Singh**, Praneeth Vepakomma, Vivek Sharma, Ramesh Raskar. "*Formal Privacy Guarantees for Neural Network queries by estimating local Lipschitz constant.*" Workshop on formal verification in machine learning at International Conference in Machine Learning, 2022

CVPR 2021 **Abhishek Singh**, Ethan Garza, Ayush Chopra, Praneeth Vepakomma, Vivek Sharma, Ramesh Raskar. "*DISCO: Dynamic and Invariant Sensitive Channel Obfuscation*" Computer Vision and Pattern Recognition, 2021.

FG 2021 Praneeth Vepakomma, **Abhishek Singh**, Emily Zhang, Otkrist Gupta, Ramesh Raskar. "*NoPeek-Infer: Preventing face reconstruction attacks in distributed inference after on-premise training*". Face and Gesture'21. (**Runner up best paper award**)

NeurIPS(W) 2020 Chaoyang He, Songze Li, Jinhyun So, Mi Zhang, Hongyi Wang, Xiaoyang Wang, Praneeth Vepakomma, **Abhishek Singh**, Hang Qiu, Li Shen, Peilin Zhao, Yan Kang, Yang Liu, Ramesh Raskar, Qiang Yang, Murali Annavaram, Salman Avestimehr. "*FedML: A Research Library and Benchmark for Federated Machine Learning.*". SpicyFL workshop at Neural Information Processing Systems 2020. (**Best paper award**)

Accomplishments and Leadership

TATA Fellow — Awarded scholarship for one year for work in digital health and privacy

Research Lead — Co-founded PrivateKit which eventually became pathcheck.org. Headed data science teams, research projects, won data science and pandemic tech competitions.

Researcher — Openmined Research team, Openmined Security and Identity team

Dev Lead — ProximityPilot App, currently deployed across MIT graduate dorms for data collection and contact tracing. See TedX MIT video here

Patents

1) Reducing leakage in distributed deep learning, patent filed with MIT.

2) Embedding private context in Google/Apple exposure notification API, patent filed with MIT

3 Secret sharing of low entropy bits, patent filed with MIT

4) Knowledge extraction in neural architecture search, pending with US patent office

5) Budgeted neural architecture search, pending with US patent office

6) Neural architecture construction using envelopenets, Patent Link

7) Lightweight malware inference architecture, Patent Link

Academic Service

Reviewer, Reviewed more than 20 conferences and journal submissions at - NeurIPS, ICML, ECCV, CVPR, ICLR, ACM Health.

Organizer, Co-organized Distributed and Private ML at ICLR'21, Crazy and Fun ideas at ICML'22, Responsibledata.ai, Trust in Pandemic Tech.

Tutorial, Organized a hands-on tutorial on Split Learning at SLDML'21.

Work Experience and Training

Aug 18-July 19 — **Research and Systems Engineer**, *Cisco*, Bangalore, India.

- Research in AutoML, Neural Architecture Search.
- Open-source efforts for ML benchmarking using MLPerf.

Aug 17-July 18 — **Cisco International Internship Program**, *Cisco*, San Jose, California.

- Worked on machine learning pipeline and systems. Worked on research problems like - intersection of Deep learning and security, AutoML.
- Contributed to **MLPerf** training workloads for the benchmarking community. Implemented one of the first implementation of transformers in PyTorch.
- Presented research work at **Cisco Annual Data Science Summit 2018, Prague, Czech Republic**.

May-June 17 — **Summer School on Information Security**, *ACM India*, VIT, Vellore, Tamil Nadu.

- Attended summer school on information and system security.
- Presented ML based network intrusion detection.

July 16 **Penetration Testing Program**, *National Security Database*, Delhi.

- Participated in 3 day bootcamp program on practical pen-testing skills and whitehat hacking.
- Finished the 8-hour pen-testing lab exam successfully.

Apr-Aug 16 **Feature Creeping and Bug Hunting**, *Google Summer of Code*.

- Worked with Nmap community for GSOC program.
- Fixed some of the major bugs in the NMAP's codebase around memory leaks, clock and asynchronous multi-threading
- Introduced features like TCP fallback, scanning decoys for IPV6, DNSSEC verification

Aug 15-May 17 **Systems and Network Assistant**, *IIIT*, Sri City, Equivalent of Teaching Assistant.

- Assisted professors and course TAs in setting up IT infrastructure for their courses.
- Managed servers for important university resources like authentication system, data backup and storage.

May-July 15 **Network and Server management**, *IIIT Hyderabad and Rekall Softwares*.

- Participated in a 3 month training and internship program focused on virtualization and automation of system administration and network management tasks.