

# Aman Priyanshu

## Graduate Student at Carnegie Mellon University

amanpriyanshu.github.io @ apriyans@andrew.cmu.edu github.com/AmanPriyanshu  
Google Scholar twitter.com/AmanPriyanshu6

## Education

Present Aug 2023	<b>Carnegie Mellon University</b> MSIT — Privacy Engineering	Pittsburgh, PA, USA
Jul 2023 Jul 2019	<b>Manipal Institute Of Technology, MAHE</b> B.Tech Information Technology with Minors in Big Data Analytics	Karnataka, India

## Professional Experience

Present Jan 2024	<b>OpenAI   Red Teaming Network, Independent Contractor</b> Participated in OpenAI led red teaming efforts to assess the risks and safety profile of OpenAI models.	Remote / San Francisco, CA, USA
Aug 2023 Aug 2022	<b>Eder Labs R&amp;D Private Limited   Privacy Engineer Intern</b> Worked on differentially private synthetic data generation for high-content tabular data and RDBMS.	Remote / Delaware, USA
May 2022 Mar 2022	<b>DynamoFL   Federated Learning Intern</b> Worked on federated recommendation systems for privately secure federated aggregation.	Remote / California, USA

## Research Experience

Present Aug 2023	<b>Privacy Engineering Research</b> [📄] <i>Independent Study   Advisor: Professor Norman Sadeh</i> Project: For prompt-engineering geared towards usable privacy & security.	Carnegie Mellon University, USA
Present Aug 2023	<b>OpenMined   Research Team</b> [📄] <i>Project Lead and Collaborator   Collaborators: Dr. Niloofar Mireshghallah</i> Project: The impact of epsilon differential privacy on LLM hallucinations.	Remote / United Kingdom
Aug 2022 Jun 2022	<b>Concordia University</b> [📄] <i>MITACS Globalink Research Intern   Advisors: Professor Wahab Hamou-Lhadj</i> Project: Exploring machine learning for anomaly detection toolkit.	Montreal, Canada

## Honours and Awards

- > Space Theme Category Winner, HackCMU, Sept 2023
- > AAAI Undergraduate Consortium Scholar, Feb 2023
- > Second Runners-Up - ShowYourSkill (Coursera), Jun 2022
- > Runners-Up - BobHacks 2021 (MetaBob API), Sept 2021
- > First Prize - HackRx by Bajaj Finserv, July 2021
- > First Prize - ACM UCM Datathon, UC Merced, May 2021

## Publications

S=In Submission, J=Journal, W=Workshop, (\* = Equal Contribution)

- [S.1] **Are Chatbots Ready for Privacy-Sensitive Applications? An Investigation into Input Regurgitation and Prompt-Induced Sanitization** [Preprint]  
[In Submission]
- [W.1] **Efficient Hyperparameter Optimization for Differentially Private Deep Learning** [PDF]  
Privacy Preserving Machine Learning Workshop at ACM CCS'21 [PPML@ACM CCS'21]
- [J.1] **Finding an elite feature for (D)DoS fast detection-Mixed methods research** [PDF]  
Journal: Computers & Electrical Engineering, Volume: 98, Pages: 107705, 2021 [Computers & Electrical Engineering'21]

Other venues of acceptances: AI4SG@AAAI'23, UpML@ICML'22, IEEE S&P'21, RCV@CVPR'21, and W-NUT@EMNLP'21.

## Skills

<b>Programming Languages</b>	Python, Java, SQL, Shell Scripting(Git & Bash)
<b>Frameworks</b>	PyTorch, Tensorflow, NLTK, Huggingface, FastAPI, Flask
<b>Relavant Coursework</b>	Prompt Engineering (17730), AI Governance (17716), Deep Learning (11785), Computer Technology Law (17562), Differential Privacy (17731), Information Security (17631), Usability (17734), Data Structures & Algorithms, OOPs, and Database Management.