LinkedIn: aman-priyanshu
GitHub: AmanPriyanshu
Research: Google Scholar

Aman Priyanshu

aman.priyanshu@learner.manipal.edu

Mumbai, India
(+91) 7738225541
Portfolio

Exploring Tech through the Lens of AI, Cyber Security and Research. My research interests lie in the field of Privacy-Preserving Machine Learning, Interpretable AI, and Deployable AI.

Education

B.Tech in Information Technology, Manipal Institute of Technology, GPA: 8.44/10.00 **Jul 2019 — Present**

Publications

1. Vijay, S. & **Priyanshu, A.** NERDA-Con: Extending NER models for Continual Learning — Integrating Distinct Tasks and Updating Distribution Shifts. *Accepted at the Updatable Machine Learning Workshop, ICML 2022* (2022).
2. Varghese, J. E., Muniyal, B. & **Priyanshu, A.** Finding an elite feature for (D)DoS fast detection—Mixed methods research. Journal: Computers & Electrical Engineering, Volume: 98, Pages: 107705. https://doi.org/10.1016/j.compeleceng.2022.107705 (2022).
3. **Priyanshu, A.**, Naidu, R., Mireshghallah, F. & Malekzadeh, M. Efficient Hyperparameter Optimization for Differentially Private Deep Learning. *Accepted at the Privacy Preserving Machine Learning Workshop, ACM CCS 2021*. https://arxiv.org/abs/2108.03888 (2021).
4. **Priyanshu, A.**, Vardhan, A., Sivakumar, S., Vijay, S. & Chhabra, N. "Something Something Hota Hai!" An Explainable Approach towards Sentiment Analysis on Indian Code-Mixed Data. *Accepted at Workshop on Noisy User-generated Text (W-NUT), EMNLP 2021* (2021).
5. Naidu, R., **Priyanshu, A.**, Kumar, A., Kotti, S., Wang, H. & Mireshghallah, F. When Differential Privacy Meets Interpretability: A Case Study. *Accepted at the Responsible Computer Vision Workshop, CVPR 2021 and Privacy Preserving Machine Learning Workshop, ACM CCS 2021*. https://arxiv.org/abs/2106.13203 (2021).
6. **Priyanshu, A.** & Naidu, R. FedPandemic: A Cross-Device Federated Learning Approach Towards Elementary Prognosis of Diseases During a Pandemic. *Accepted at the Machine Learning for Preventing and Combating Pandemics and the Distributed and Private Machine Learning Workshops, ICLR 2021*. https://arxiv.org/abs/2104.01864 (2021).

Work Experience

Privacy Engineer Intern **Aug 2022 — Present**
Eder Labs R&D Private Limited Delaware, USA

- Working on differentially private synthetic data generation for high-content tabular data and relation database systems.
- Conducted research towards vertical federated learning on financial data.

Federated Learning Intern **Mar 2022 — May 2022**
DynamoFL California, USA

- Worked on federated recommendation systems for privately secure federated aggregation.

Technical Head **Jun 2020 — Aug 2022**
Cryptonite Student Project

- Technical Head of Cryptonite - the official Cyber Security Student Project of MIT, Manipal. Participated in multiple CTF competitions, ranked 12th in India on CTFtimes (2022). Developed and led research projects on Privacy-Preserving Machine Learning.

Research Experience

MITACS Research Intern **May 2022 — Aug 2022**
Concordia University Quebec, Canada

- Worked under the supervision of Professor Wahab Hamou-Lhadj on reinforcing anomaly detection model for online, adaptable deployment with marginal false alarms.

Expertise Sub-Head, Artificial Intelligence **Feb 2021 — Sep 2022**
Research Society Manipal Karnataka, India

- Leading and mentoring peers within RSM for Artificial Intelligence, with a focus on integrating machine learning and privacy. Research Society Manipal is an organization that focuses on research in different fields.

Projects

AdaptKeyBERT **Oct 2022**
- Built a python library, integrating semi-supervised attention for creating a few-shot domain adaptation technique for keyphrase extraction.
- Extended the work by allowing zero-shot word seeding, allowing better performance on topic relevant documents.

NERDA-Con **May 2022**
- Created NERDA-Con, a python package for training NER models with LLM bases for continual learning.
- Achieved an improvement of +4.67% for training over distribution shifts and +13.66% for generalizing across tasks compared to baseline models.

DP-SDV **Jun 2022**
- Creating a python library for Differential Privacy securing Synthetic Data Generation for tabular, relational and time series data.

DP-HyperparamTuning **Aug 2021**
- DP-HyperparamTuning offers an array of tools for fast and easy hypertuning of various hyperparameters for the DP-SGD algorithm. We proposed a novel, customizable reward function that allows users to define a single objective function for establishing their desired privacy-utility tradeoff.

Augmented Face Detection API for Professional Image Approval **Jul 2021**
- The app performs obstruction detection, spoof detection, blur detection and environment approval. Utilized Deep Neural Networks and Genetic Algorithms to achieve these goals in low computational time. The project won 1st place in *HackRx 2.0 by Bajaj Finserv.*

DeCrise **May 2021**
- DeCrise is an online platform that acts as an aggregator for public support/utility services which uses continual-federated-learning to create a quick response information retrieval system during a natural disaster. The project won 1st place in *The ACM UCM Datathon*.

Awards & Extra-Curricular

Felasa-Initiative **Aug 2022**
- Felasa-Initiative is The Feminine Law Safety Awareness Initiative. Our vision entails legally empowering women (both educated and illiterate) ignorant of their rights to access and demand justice.

Second Runners-Up - #ShowYourSkill (Coursera) **Jun 2022**
- Came second runners-up in #ShowYourSkill where we participated in the Research & Reports Track and creating a NLP augmented Machine Learning Application for women safety.

Runners-Up - BobHacks 2021 (MetaBob API) **Sep 2021**
- Came runners-up in BobHacks where we built a pattern recognition API built on top of the MetaBob API. The API is able to assist users in tracking common errors and delivers pattern recognition on the MetaBob API.

First Prize - Code Innovation Series - associated with GitHub **Aug 2021**
- Innovation Series Hackathon was the hackathon organized by by Manipal Institute of Technology.
- Employed Document-Embedding for measuring contextual similarity between multiple pages and given search-queries.

First Prize - HackRx by Bajaj Finserv **Jul 2021**
- HackRx is the Annual Hackathon hosted by Bajaj Finserv.
- Used Deep Learning and Classical Image processing to achieve a face verification and profile-rank estimation task. The methodology out-performed classic Deep Learning methods. Created an API for the same.

First Prize - ACM UCM Datathon - UC Merced **May 2021**
- Won the ACM UCM Datathon, built DeCrise, an online platform that acts as an aggregator for public support/utility services for fast-response during a major crisis or disaster.

First Prize - Community & Civic Engagement track of CalHacks Hackathon **Apr 2021**
- Won under the Community & Civic Engagement track of CalHacks Hackathon organized by UC Berkeley.
- Built Voix, an anonymous platform for uplifting communities and promoting civic participation. It is a social media platform that utilizes privacy-enabled machine learning to recover ideas affecting communities and bring them to the top of our platform while conserving user identity.

Runners-Up - IEEE BigMM Data Challenge - IEEE Grand-Challenge **Aug 2020**
- Came runners-up in IEEE Grand-Challenge for harassment detection on tweets. Utilized Elementary Classifiers for Sentiment Analysis.
- The team was invited to present a paper in IEEE Sixth International Conference on Multimedia Big Data (BigMM).

Technical Skills

Programming	Python, Java, C, C++, MATLAB, Julia, Go, Latex
Technical Skills	PyTorch, TensorFlow, Scikit-Learn, Numpy, Cuda, FastAPI, Flask