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

Aman Priyanshu

apriyans@andrew.cmu.edu

Mumbai, India
(+91) 7738225541
Portfolio

Exploring Tech through the Lens of AI, Cyber Security and Research. I am deeply passionate about Deep Learning, Cyber Security and the Research bringing together these two vast fields. My research interests lie in the field of Privacy-Preserving Machine Learning, Deep Learning, Reinforcement Learning, Large Language Models, and Cyber Security.

Education

MSIT - Privacy Engineering, Carnegie Mellon University — **Aug 2023 — Present**

B.Tech in Information Technology, Manipal Institute of Technology — **Jul 2019 — Jul 2023**

Research Experience

AAAI Undergraduate Consortium Scholar — **Feb 2023**
Association for the Advancement of Artificial Intelligence — DC, USA

- Presented my work on Fairness induction using Super-masking of member networks in a Federated Environment.

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.

Undergraduate Research Assistant — **May 2021 — Present**
Manipal Institute of Technology — Karnataka, India

- Working under the supervision of Professors Balachandra Muniyal and Nisha P. Shetty on machine learning approaches to solve problems in the field of selective encryption and privacy-preserving machine learning.

Reviewer — **Sep 2022 & Aug 2021**
BlackboxNLP 2022 & 2021

- Reviewed papers for BlackboxNLP 2022 & 2021, collocated with EMNLP2021. The goal of this workshop was to bring together people who are attempting to peek inside the neural network black box.

Expertise Sub-Head, Artificial Intelligence — **Feb 2021 — Present**
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.

Industrial Experience & Positions of Responsibility

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 — **March 2022 — May 2022**
DynamoFL — California, USA

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

Technical Head — **Jun 2021 — Present**
Cryptonite Student Project

- Technical Head of Cryptonite - the official Cyber Security Student Project of MIT, Manipal. Participated in multiple CTF competitions, ranked 18th in India on CTFtimes (2021). Developed and led research projects on Privacy-Preserving Machine Learning.

Machine Learning and Web Crawling Intern — **Jan 2020 — Feb 2020**
Oniria Pets

- Interned at Oniria pets as a Machine Learning and Web Crawling Developer for Data Extraction and Management. Employed BERT for precise feature extraction pertaining to hotel prices, billing systems, locations etc. on data scraped from Hotel Websites. Used Selenium and Scrapy for extraction.

Google Code In mentor **Dec 2019 — Jan 2020**

TensorFlow User Group (TFUG)

- Mentored at Google Code-in for TensorFlow User Group (TFUG) - GCI'19.

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.**, Shastri, S. & Medicherla, S. S. ARLIF-IDS – Attention augmented Real-Time Isolation Forest Intrusion Detection System. *Accepted at Poster session at the 43rd IEEE Symposium on Security and Privacy* (2022).
4. **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).
5. **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).
6. 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).
7. **Priyanshu, A.**, Sinha, M. & Mehta, S. Continual Distributed Learning for Crisis Management. *Accepted at the 3rd Workshop on Continual and Multimodal Learning for Internet of Things, IJCAI 2021*. https://arxiv.org/abs/2104.12876 (2021).
8. **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).
9. **Priyanshu, A.**, Das, V. R., Rajiv Moghe, S., Rathod, H., Medicherla, S. S., Shail Chhabra, M. & Shastri, S. Stance Classification with Improved Elementary Classifiers Using Lemmatization (Grand Challenge). *2020 IEEE Sixth International Conference on Multimedia Big Data (BigMM).* https://www.doi.org/10.1109/BigMM50055.2020.00077 (2020).

Technical Skills

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

Projects

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 **June 2022**

- Creating a 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.

Hexa Lite **Aug 2021**

- Created an unsupervised machine learning to extract contextually similar texts. The project was used in indexing Academic Literature, Law Precedents, and Financial Records. The project won *Code Innovation Series* - a Hackathon in association with *GitHub*.

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*.

Voix **Apr 2021**

- A social-media platform employing machine learning and differential privacy to promote civic engagement while protecting user-privacy. The project won under the *Community & Civic Engagement for UC Berkeley's CalHacks Hackathon*.

Awards

Second Runners-Up - #ShowYourSkill (Coursera) **June 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.

Runners-Up - Paper Presentation - IEEE SBM Manipal **Apr 2021**

- Presented a preliminary investigation of Federated Learning integrated with Continual Learning for Crisis Management.

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.

Furniture Identification - IECSE x VISION **Sep 2020**

- Employed skip-connections to generate high-performance model for furniture identification.

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).

Scholarship Recipient - Intel Labs **Jan 2020**

- Honored to be selected as one of the recipients of the Intel Edge AI Scholarship Program.
- Learnt about Machine Learning Implementation on the Edge.