

# AMAN PRIYANSHU

**in** LinkedIn (linkedin.com/in/aman-priyanshu-050473191)

Personal Website (amanpriyanshu.github.io)

☎ (+91) 7738225541 ✉ amanpriyanshusms2001@gmail.com

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. Exploring opportunities to learn and grow.

**Areas of Interest** Privacy Enabled Machine Learning, Deep Learning, Reinforcement Learning, Spiking Neural Networks and Cyber Security.

## EDUCATION

---

**Manipal Institute of Technology, Manipal**  
B.Tech in Information Technology

*July 2019 – Present*

## POSITIONS OF RESPONSIBILITY

---

**The Research Society MIT**  
*Expertise Sub-Head, Artificial Intelligence*

*Feb 2021 – Present*

- Leading and mentoring within RSM for Artificial Intelligence, with a focus on integrating machine learning and privacy. A member of the Research Society, an organization that focuses on the research in different fields, both interdisciplinary and otherwise.

**Cryptonite Student Project**  
*Technical Head*

*June 2020 – Present*

- Technical Head of the Cyber Security Student Project of Manipal, Cryptonite. Participated in multiple CTF competitions, currently (2020) ranked as 25th in India on CTFtimes. Developed and led research projects on Privacy Preserving Machine Learning.

**Oniria Pets**  
*Machine Learning and Web Crawling Intern*

*Jan 2020 – Feb 2020*

- 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.

## RESEARCH EXPERIENCE AND PUBLICATIONS

---

**When Differential Privacy Meets Interpretability: A Case Study.**

*Jun 2021*

- In this paper we present the interpretability-privacy trade-off of DP trained models and provide the first benchmark of the same. The paper was accepted in *Responsible Computer Vision Workshop at CVPR'2021*.

**FedPandemic: A Cross-Device Federated Learning Approach Towards Elementary Prognosis of Diseases During a Pandemic**

*May 2021*

- In this paper, we presented FedPandemic, a novel noise implementation algorithm integrated with cross-device Federated learning for Elementary symptom prognosis during a pandemic, taking COVID-19 as a case study. The paper was accepted in *Distributed and Private Machine Learning Workshop at ICLR (2021)* and in *ICLR 2021 Workshop on Machine Learning for Preventing and Combating Pandemics*. The project presents a novel application of PPML for disease prognosis.

## Continual Distributed Learning for Crisis Management

May 2021

- Presented our paper on continual and distributed learning for Crisis Management, which employed model regularization to alleviate catastrophic forgetting and federated learning for distributed learning. We came runners up in the *Paper Presentation event at IEEE-SBM*.

## Stance Classification with Improved Elementary Classifiers Using Lemmatization (Grand Challenge)

Sept 2020

- Came Runners Up in the *IEEE BigMM Data Challenge*, we came up with a model for accurate classification of sensitive tweets for the #MeToo movement. We worked on a highly biased dataset by introducing concepts of under-sampling and lemmatization to improve performance of elementary classifiers which enabled low-resource deployment.

## RELEVANT PROJECTS

---

### DeCrise

May 2021

- DeCrise is an online platform that acts as an aggregator for public support/utility services for fast-response during a major crisis or disaster. We bring together the concepts of both continual and federated learning to create a volunteer-supported, learning system for the quick response and integral information retrieval during a natural disaster. The project won 1st place in *The ACM UCM Datathon*.

### Voix

Apr 2021

- A social-media platform for uplifting communities and promoting civic participation. Created and deployed a social media platform, which utilized machine learning and differential privacy to promote civic engagement while protecting user-privacy. We created a contextual-similarity based recommender system to promote positive reinforcement while still promoting healthy debates. The project won under *Community & Civic Engagement for UC Berkeley's CalHacks Hackathon*.

### Neural Embedding of Textual Data into Audio

Jul 2020

- Created a Deep Learning based Neural Embedding Model for encoding Textual Data (Plain Text) and an Audio File (Method of Transfer) into a single Audio File (Cypher Text).

## AWARDS AND HONOURS

---

- First Place in The ACM UCM Datathon (UC Merced)
- Winner under Community & Civic Engagement for UC Berkeley's CalHacks hackathon
- IEEE BigMM Data Challenge Runner's Up
- First Prize Winner by HackRx - Bajaj Finserv
- Intel Edge AI Scholarship Recipient
- Runner-Up in Paper Presentation at IEEE-SBM

## TECHNICAL STRENGTHS

---

### Programming Languages/Frameworks

Python, Julia, Java, C++, Go, MongoDB, PyTorch, Tensorflow, keras, Flask, Django, Linux, Windows, Android

### Languages

English, French

## RELEVANT COURSEWORK

---

- Our Privacy Opportunity by OpenMined
- Deep Learning Specialization by deeplearning.ai
- TensorFlow in Practice Specialization by deeplearning.ai
- Introduction to Cyber Attacks by NYU