AMAN PRIYANSHU

amanpriyanshusms2001@gmail.com ⋄ linkedin.com/in/AmanPriyanshu ⋄ amanpriyanshu.github.io

EDUCATION

MSIT - Privacy Engineering, Carnegie Mellon University — Aug 2023 - Expected Dec 2024
School of Computer Science

BTech in Information Technology, Manipal Institute of Technology — Jun 2019 - Jul 2023
Dept. of Information & Communication Technology — **Cum. GPA: 8.43/10**

EXPERIENCE

Privacy Engineer Eder Labs R&D Private Limited — Aug 2022 — Jul 2023

- Working on private synthetic data generation for RDBMS & semi-supervised domain adaptation for KeyBERT.
- Created two public python libraries, DPSDV & AdaptKeyBERT, for the same.
- Working on prompts for creating a personalized conversational LLM with privacy awareness.

MITACS Research Intern Concordia University — May 2022 — Aug 2022

- Worked on reinforcing anomaly detection model for online, adaptable deployment with marginal false alarms.

Federated Learning Intern DynamoFL — March 2022 — May 2022

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

PUBLICATIONS

1. **Priyanshu, A.**, Vijay, S., Kumar, A., Naidu, R. & Mireshghallah, F. Are Chatbots Ready for Privacy-Sensitive Applications? An Investigation into Input Regurgitation and Prompt-Induced Sanitization (2023).
2. Varghese, J. E., Muniyal, B. & **Priyanshu, A.** Finding an elite feature for (D)DoS fast detection—Mixed methods research. Journal: Computers & Electrical Engineering, Elsevier, 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. 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).
5. **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* (2021).

PROJECTS

DeCrise — Link

- DeCrise, a public support platform employing continual-federated-learning for IR during natural disasters. Won 1st place in *The ACM UCM Datathon* (Technology: Privacy Engineering).

Voix — Link

- An anonymizing civic engagement platform that won under the *Community & Civic Engagement for UC Berkeley's CalHacks Hackathon* (Technology: Privacy Engineering).

SKILLS

Languages & Frameworks — Python, Julia, Java, C++, PyTorch, TensorFlow, HuggingFace, FastAPI

EXTRA-CURRICULAR ACTIVITIES

AAAI Undergraduate Consortium Scholar [Link]	Feb 2023
Expertise Sub-Head, Artificial Intelligence, Research Society Manipal	Feb 2021 — Sep 2022
Technical Head, Cryptonite Student Project	Jun 2021 — Sep 2022
Second Runner's Up, #ShowYourSkill (Coursera)	June 2022
Awarded a research seed grant for UG & PG Students	Feb 2022
First Prize, Code Innovation Series - associated with GitHub	Aug 2021