SHUBHAM MALAVIYA

+91 8758648003 ⋄ Pune, Maharashtra
smalaviya311@gmail.com ⋄ LinkedIn ⋄ Google Scholar

ABOUT

I am a researcher with a passion for applying AI to various domains to enhance human productivity. Specializing in AI application within Cybersecurity for more than 4 years, I have authored two published papers and filed a patent as the lead author, emphasizing Natural Language Processing integration.

EDUCATION

M.Tech, Dhirubhai Ambani Institute of Information and Communication Technology, Gujarat 2019
Specialization in Machine Learning

CGPA: 8.45

B.E., L.D. College of Engineering, Gujarat 2017
CGPA: 8.41

SKILLS

Technical Skills	Machine Learning & Deep Learning, Natural Language Processing, Federated Learning, Data Interpretation, Prompting, Python, TensorFlow, PyTorch
Soft Skills	Research & Experimental Design, Continuous Learning, Adaptability, Technical Writing

EXPERIENCE

Researcher Aug 2019 - Present
Tata Consultancy Services *Pune, Maharashtra*

- **Classify Enterprise Documents Based on the Content Sensitivity.**
  I utilized state-of-the-art deep learning techniques to develop a novel text classification solution. A key challenge we faced was the sensitivity of the data and the need for Non-Disclosure Agreements (NDAs) with clients, which made acquiring suitable training data and conducting comprehensive research quite challenging.
- **Privacy Preserving AI**
  As the principal investigator, I devised a privacy-preserving solution for training deep learning models. Our approach utilized federated learning, allowing collaborative model learning without users sharing their data with a centralized server. We considered a scenario where users have unlabeled data and the server has curated labeled data.
  We introduced FedFAME, a framework for federated semi-supervised learning, which eliminates the need for data augmentation. We presented this work at the prestigious **38th ACM/SIGAPP Symposium on Applied Computing (SAC), 2023**. We have **filed a patent** for this innovative solution.
- **Reducing Communication Overhead in Federated Learning**
  As the principal investigator, I explored the feasibility of Parameter Efficient FineTuning (PEFT) methods to reduce communication overhead in federated learning while maintaining a strong model performance in supervised and semi-supervised settings. Additionally, we conducted an extensive analysis to evaluate the transferability of PEFT methods in federated learning across different NLP tasks.
  Our noteworthy contribution has been accepted at the **Second Conference on Lifelong Learning Agents (CoLLAs) 2023**.
- **Influence Based Defense Against Data Poisoning Attacks in Online Learning**
  As an integral part of this project, I actively contributed by implementing and validating specific components of the experimental process, while also assisting in the development of the research paper.
  Our extensive efforts culminated in the successful publication of our research paper in the esteemed **14th International Conference on COMmunication Systems & NETworkS (COMSNETS) 2022**.

ACHIEVEMENTS

- Four TCS Citation Awards
- One IP Creation Award
- Service & Commitment Award
- Certification of Appreciation from SONY for featuring in The Top Exhibited Photographs in 2022.