SHUBHAM MALAVIYA

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

ABOUT

I am a researcher with a passion for applying AI across diverse domains to enhance human productivity. My primary expertise lies in the application of AI within the field of Cybersecurity, where I have accumulated over four years of specialized experience. I have authored two published papers and filed a patent as the lead author, with a particular emphasis on the integration of Natural Language Processing techniques.

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, Generative AI, Data Interpretation, Python, TensorFlow, PyTorch
Soft Skills	Research & Experimental Design, Continuous Learning, Adaptability, Technical Writing

ACHIEVEMENTS

- Served as **review committee member** for The 39th ACM/SIGAPP Symposium On Applied Computing
- **Patents and Publications**
  - **Primary inventor** in a Patent **filed in India, EPO and US** for our work on privacy-preserving sensitive data classification
  - **Poster** *DroPacter: Compacter-based Tuning with Layer Freezing in Pre-trained Language Model* accepted in The 39th ACM/SIGAPP Symposium On Applied Computing
  - **Paper** *Reducing Communication Overhead in Federated Learning for Pre-trained Language Models Using Parameter-Efficient Finetuning* accepted and presented in The Second Conference on Lifelong Learning Agents
  - **Paper** *FedFAME: A Data Augmentation Free Framework based on Model Contrastive Learning for Federated Semi-Supervised Learning* accepted and presented in The 38th ACM/SIGAPP Symposium On Applied Computing
  - **Paper** *Influence based defense against data poisoning attacks in online learning* accepted in The 14th International Conference on COMmunication Systems & NETworkS (COMSNETS)
- Five **TCS Citation** Awards
- One **Intellectual property (IP)** Creation Award
- Service & Commitment Award
- Earned **Google Cloud Skill Badge** for Generative AI Fundamentals & Generative AI with Vertex AI: Text Prompt Design
- Certification of Appreciation from **SONY** for featuring in the **Top Exhibited Photographs** in 2022

EXPERIENCE (4.3 YEARS)

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

- **Classify Enterprise Documents Based on the Content Sensitivity**
  - I explored state-of-the-art deep learning techniques to develop a novel text classification solution for identifying sensitive data. 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.
  - I evaluated methods such as Latent Dirichlet Allocation (**LDA**), **BERT** and Hierarchical Attention Networks (**HAN**) on **WikiLeaks** dataset.
  - **Technologies used:** Python, TensorFlow, NLTK, Matplotlib
- **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 evaluated models based on **Bidirectional LSTM** (for texts) and **Convolution** (for images) on **non-i.i.d. data**.
  - This work led to the publication of **1 research paper** and creation of **1 patent**.
  - **Technologies used:** Python, TensorFlow, Flower, Matplotlib
- **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.
  - We **finetuned BERT-Base** model employing techniques such as **Prefix tuning, Adapter, BitFit and LoRA**, and evaluated the model performance on six datasets from **GLUE** benchmark. Remarkably, we successfully reduced the communication **cost from 420 MB to $<$ 50 MB**. This work led to the publication of **1 research paper**.
  - **Technologies used:** Python, PyTorch, Transformers, OpenDelta, Flower, Matplotlib
- **Compacter-based Finetuning of Pre-trained Language Models (PLMs) in CyberSecurity**
  - We assessed pre-trained language models (PLMs) on cybersecurity tasks, showcasing that DroPacter-based models achieved comparable performance to full model fine-tuning with only **0.06% of total parameters**, and trained **40% faster**. This work led to the publication of **one poster**, with my contributions focusing on experiment design, results, and content coherence validation.
  - **Technologies used:** Python, PyTorch, Transformers, OpenDelta, Flower, Matplotlib
- **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 **14th International Conference on COMmunication Systems & NETworkS (COMSNETS) 2022**.

- **Exploring The Applicability of Generative AI in Cybersecurity**
  - In light of the latest developments in Generative AI, our team is presently investigating ways to enhance the efficiency of existing cybersecurity systems through its application.
- Conducted **20+ interviews**

ACADEMIC PROJECTS

- **Defending Machine Learning Models against Adversarial Attacks Using GANs (M.Tech.)**
  - Our proposal involves incorporating a similarity measure between images in the training process of Generative Adversarial Networks (**GANs**). We explored the impact of various similarity measures on the robustness of the trained model against adversarial attacks. Throughout the training phase, the Generator aims to replicate the distribution of real data, while the trained Discriminator is employed to identify adversarial images.
  - **Technologies used:** Python, TensorFlow
- **Customizing the Open Source Automatic Time Table Generation Tool - FET (B.E.)**
  - We utilized FET, an open-source timetable generation tool, and made certain modifications to enhance its functionality. My specific responsibility involved identifying the connections between the graphical user interface (GUI) and function calls in C++ codebase. Additionally, I converted an Excel file into XML and populated entries in the FET tool by extracting data from that XML file.
  - This modified tool was successfully **employed by the I.T. department** at L.D. College of Engineering for generating the timetable for the **year 2016**.