Sakshi Pandey

Roll No. 24M2115 +91 88793722210
sakshipandey@cse.iitb.ac.in linkedin.com/in/thesakshipandey github.com/thesakshipandey

Education

Indian Institute of Technology, Bombay 2024 - Present
MS by Research in Computer Science (Upto Sem1: 9.29 / 10.00) *Mumbai, Maharashtra*

University of Mumbai 2019 - 2023
Bachelor of Engineering in Computer Engineering (GPA: 8.86 / 10.00) *Mumbai, Maharashtra*

Experience

Bombay Stock Exchange LTD Sept 2021 – Oct 2021
Cybersecurity Intern *Mumbai, Maharashtra*

- **Risk and Vulnerability Analysis**: Gained hands-on experience in identifying and assessing risks, faults, and vulnerabilities within systems.
- **Threat Detection and Response**: Worked with IBM Watson to detect and mitigate security threats using IBM QRadar.
- **Honeycomb Trapping**: Learned and implemented Honeycomb trapping techniques to enhance security measures against potential threats.

Projects

Reinforcement Learning in Side-Channel Attacks | *R&D under Prof. Shivaram K. and Sayandeep S.*

- **Automated CNN Design**: Built a Q-Learning agent that sequentially composes 1D-CNN layers (Conv, Pool, BatchNorm, FC, Softmax) with tunable hyperparameters to optimize profiling SCA models.
- **SCA-Specific Reward Engineering**: Designed composite reward functions combining guessing-entropy convergence at multiple trace budgets and validation accuracy — and a variant adding a model-size penalty — to drive the agent toward compact, high-performance networks.
- **Empirical Evaluation**: Integrated the RL loop with TensorFlow/Keras, ran ¿2 700 architecture trials on ASCAD, DPAContest v4 and CHES CTF datasets, and discovered lightweight CNNs that match or exceed state-of-the-art key-recovery performance.

Signboard Translation from Vernacular Languages | *Course Project: Foundation of Machine Learning*

- **Text Detection and Extraction**: Implemented Faster R-CNN for precise text detection and utilized EasyOCR for extracting text from various regional scripts in signboard images.
- **Transliteration**: Developed an attention-based GRU Encoder-Decoder model for transliteration, converting extracted Hindi text into English while preserving context and meaning.
- **Preprocessing**: Preprocessed images to improve OCR accuracy and ensure compatibility with neural models.

Red Teaming in Large Language Models (LLMs) | *Project of CFILT Lab*

- **Multilingual Analysis**: Explored vulnerabilities in LLM safety filters, focusing on Indic languages like Telugu, Bengali, and Marathi, with custom annotations.
- **Prompt Manipulation**: Used Mixtral to bypass safety constraints by leveraging multilingual and context-based tactics.
- **Custom Prompt Templates**: Designed and developed our own prompt templates to bypass safety filters in LLMs, focusing on multilingual challenges in Indic languages.

Movie Recommendation System | *Course Project: Software Lab*

- **Hybrid Filtering Approach**: Designed a personalized recommendation engine using Singular Value Decomposition (SVD) for collaborative filtering and cosine similarity for content-based filtering, merging them for hybrid recommendations.
- **Sentiment Analysis**: Performed analysis on user reviews scraped from movie platforms like IMDb, utilizing NLP techniques for better insights.
- **EDA & Dataset Integration**: Combined the MovieLens and Netflix datasets to improve recommendation accuracy through data preprocessing, feature engineering, and exploratory data analysis.

Embedding Generation from Scene Graphs | *RnD under Prof Ganesh R.*

- Implemented a pipeline inspired by Graph Convolutional Networks (GCN) and Graph Attention (GAttn) techniques to transform scene graphs into rich embeddings.
- Incorporated ideas from the paper *"Image Generation from Scene Graphs"* to process and represent objects and relationships in a structured graph format.
- Developed a dataset of 125 images with their corresponding scene graphs and extracted encodings using Vision Transformer (ViT) with 224-pixel patches.
- Employed visualization techniques like t-SNE to analyze and evaluate the quality of the learned embeddings.

Decentralized Storage System using Blockchain Technology | *Final Year BE Project*

- **Conceptualization and Design**: Designed a decentralized storage system leveraging blockchain technology to ensure data integrity, security, and accessibility.
- **Implementation**: Developed and implemented smart contracts to manage data transactions and storage operations.
- **Security Enhancement**: Incorporated cryptographic techniques to secure data and ensure tamper-proof records.

Technical Skills

Languages: Java, Python, C, C++, Solidity, SeD, AWK, Bash.
Technologies: Flask, Bootstrap, Numpy, Pandas, Tensorflow, PyTorch.
Concepts: Compiler, Operating System, Web Development, Encryption, Decryption, CyberSecurity, Database Normalization, Machine Learning, Neural Networks, Attention, Word2Vec, Reinforcement Learning, Side Channel Attacks, Encoder, Decoder.

Achievements & Certifications

- **Published Research Paper**: Authored and published a research paper on "Decentralized Storage System using Blockchain Technology" at IEEE ASIACON'23.
- **Google Developer Student Club Lead**: Became the first Google DSC Lead at my institute in 2022, organizing and leading various tech workshops and events.
- **Kaggle Competition Winner**: Secured 1st place in both Kaggle competitions conducted as part of the CS725 (Foundations of Machine Learning) course at IIT Bombay.
- **Reliance Foundation PG Scholar**: Awarded the prestigious Reliance Foundation Postgraduate Scholarship, given to only 100 students across the country for academic excellence and leadership.

Hobbies

Sports: Basketball, Badminton, Chess
Academia: Read, Code