(+91)-8588038790
Gurugram, India
satya29m3@gmail.com

Satyadwyoom Kumar

Satyadwyoom.com
github/satyadwyoom
linkedin/satyadwyoom

Education

University of Delhi (NSIT) **Aug 2018 - May 2022**
B.E., Electronics and Communication Engineering
CVPSK Scholar (Awarded to Top 10 Students)
Thesis: Introducing temporally consistent weather conditions in aerial videos using LSTM & Cycle-GAN.
Coursework: Computer Programming, Data Structures and Algorithms, Pattern Recognition, Image Processing.

Industry Experience

Bain & Company **Oct 2024 - Present**
Data Scientist - II

OYO Rooms **Jul 2022 - Sep 2024**
Data Scientist - II — Dynamic Pricing, LLMs, Stuck Classification, EDA

- Engineered a statistical model for dynamic pricing, leading to a reduction in operation costs by $28K/month.
- Developed method employs a cost/impact-based binary search algorithm on price bucketed escalations to predict optimal prices within a constrained overhead cost.
- Developed and deployed an XGBoost classifier (f1 score: 88%) on AWS-EC2 using Python, FastAPI, and PySpark to predict booking denials. Utilized SMOTE for class imbalance. Enhanced booking realization by 20%.
- Developed a root cause analysis model from customer escalations using SQL leading to $96K savings.
- Performed EDA across 10K+ data points daily to guide initiatives for improving customer experience.
- Utilized K-Means clustering to identify anomalous properties operating in premium product category.
- Utilized LLMs to analyze and perform zero-shot classification on customer reviews (Acc: 85%).

Dell **Jan 2022 - Jun 2022**
Data Scientist — Text Transformation using NLP

- Engineered a Bag of Words + Cosine Similarity model to eliminate redundant terms from scraped data.
- Achieved a 24x speedup to check the competitiveness of Dell products w.r.t competitors without drop in accuracy.
- Optimized data pipelines for training machine learning models by developing automated web crawlers to fetch data, as well as a Python+SQL module to structure and store normalized data for downstream tasks.

Research Experience

University of British Columbia, Canada **Dec 2020 - Nov 2023**
Advisor: Prof. Apurva Narayan — Adversarial ML, GAN-Inversion, Visual Fashion Recommendation

- Developed a generative adversary that improves robustness of CNNs by generating adversarial perturbations by 11%.
- Proposed adversary maximizes distributional divergence while maintaining perturbation diversity.
- Developed a certified defense framework with a novel Gaussian noise addition procedure for defending black-box CNNs.
- Developed an algorithm that utilizes GAN-Inversion principles to optimize a latent vector, which when passed through a generator provides vendors with product-level visual modifications for improved preference across a set of users.
- Works published at **ICPR-2022, IEEE-IJCNN-2022**.

University of Delhi-(NSIT) **Aug 2021 - May 2022**
Advisor: Prof. Amit Singhal — GANs, Aerial Video Generation

- Developed a generative approach to produce different weather translations for a given aerial video.
- Heuristically modified CycleGAN (Deep-ResNet) architecture and introduced another discriminator (real/fake prediction) to compensate for image data scarcity with varied weather conditions from an aerial perspective.
- Achieved temporal coherency in translated videos via LSTM-based discriminator.

National University Singapore **Jun 2021 - Nov 2021**

Advisor: Prof. Hongliang Ren — Surgical Workflow Recognition

- Developed a lightweight multi-task learning model for robotic arm-based surgical workflow recognition.
- Proposed method utilizes a pretrained ResNet18 with LSTMs to analyze robotic arm interactions over time.
- Our method gave individual attention to the physical parameters of both the left and right arms of the robot.
- Work published at **Journal of Computer Methods and Programs in Biomedicine**.

IIIT-Delhi **Jul 2020 - Jan 2021**

Advisor: Prof. Arun Balaji Buduru — CNNs, BlackBox Optimization, Driver State Prediction

- Developed a black-box optimized physical adversarial patch, capable of fooling driver state detection systems.
- Analyzed the effect of adversarial patches while performing a realtime vision-based adversarial patch attack.
- Implemented a driver-state detection system utilizing multiple features such as driver facial expressions (using VGGNet) and hand orientation (using segmentation maps generated from Mask R-CNN) (Acc: 91%).

Publications

1. **Satyadwyoom, Kumar** and Apurva Narayan. Introducing Diversity in Feature Scatter Adversarial Training via Synthesis. In *26th International Conference on Pattern Recognition (ICPR)*, pages 3069–3075. IEEE, 2022 [Published]
2. **Satyadwyoom, Kumar** and Apurva Narayan. Towards Robust Certified Defense via Improved Randomized Smoothing. In *International Joint Conference on Neural Networks (IJCNN)*, pages 1–8. IEEE, 2022 [Published]
3. Arnaud Huaulmé, Kanako Harada, Quang-Minh Nguyen, Bogyu Park, Seungbum Hong, Min-Kook Choi, Michael Peven, Yunshuang Li, Yonghao Long, Qi Dou, **Satyadwyoom, Kumar**, Hongliang Ren, et al. Peg Transfer Workflow recognition challenge report: Do multimodal data improve recognition? *Computer Methods and Programs in Biomedicine*, 236:107561, 2023 [Published]
4. **Satyadwyoom, Kumar**, Abhijit Sharma, and Apurva Narayan. GAN Inversion and Shifting: Recommending product modifications to sellers for better user preference. *PeerJ*, 2024 [Under Review]
5. **Satyadwyoom Kumar**, Saurabh Gupta, and Arun Balaji Buduru. BB-Patch: BlackBox Adversarial Patch-Attack using Zeroth-Order Optimization. *arXiv*, 2024 [Preprint]

Projects

Personal WhatsApp Message Responder — ChatGPT, LLMs

- Utilised Selenium to fetch and send messages from/to WhatsApp chats.
- Further introduced the ability to fetch messages from a particular person in a group chat.
- Extracted messages are then used to generate a response using GPT-3.5.

NLP Tasks - using Transformers — Llama3, GPT-2, BERT, SVM, Random Forest, LSTMs

- Fine-tuned BERT leading to an improvement of 7% on sentiment analysis task for airline tweets.
- Implemented transfer learning on GPT-2 to tackle text-entailment problem.
- Fine-tuned Distil-BERT on SQuAD dataset for question/answering task (f1: 88%).
- Built a web interface using Streamlit+LangChain, incorporating Llama3 to generate insights from tabular data.
- Engineered and deployed a machine learning-based Reddit post flair detection web app on Heroku.
- Fetched 1500+ unique Reddit posts for a variety of flairs appearing on r/india using PRAW API.
- Employed preprocessing techniques: Stemming/Lemmatization to bring word tokens to their root form.
- Tested a variety of ML models: Random Forest (f1: 67% Acc: 68%), Support Vector Classifier (f1: 68% Acc: 68%).
- Further improved the flair prediction performance using BERT (f1: 75% Acc: 76%).

Graph Representation Learning Tasks — Graph-Conv, Graph-Attention

- Utilized Graph architectures to detect whether a text review is computer generated or human written.
- Performed dependency parsing to instill grammatical syntax knowledge in the trained model. (f1: 91%).
- Built a transaction graph with transaction similarity as edge-weights for credit fraud prediction.
- Utilized graph models for fraud detection: Graph Conv (f1: 80%), Graph Attention (f1: 82%)

Reinforcement Learning For Control Problems — Q-Learning, DDPG, Cross-Entropy Method, CNNs

- Developed agents such as soccer and tennis players, bipedal walker, lunar lander using Q-learning, DDPG and CEM.
- Collected 2+ hrs video data along with steering controls by driving a car in GTA San-Andreas.
- Initially trained a ResNet-18 model to simulate a self-driven car in the game.
- Further utilized Deep-Q learning to improve the precision of predicted controls in the simulated car.

Time Series Forecasting for Stock Prices — ARIMA, SARIMAX, MLPs

- Developed and tested models for forecasting stock prices of leading technology companies (Nvidia, Microsoft, Apple) using real-time data from the Yahoo Finance API.
- Evaluated models to forecast prices over the next 30 days, utilizing a 30-day historical data window: ARIMA (RMSE: 69.2), SARIMAX (RMSE: 88.3), and Multi-Layer Perceptron (MLP) (RMSE: 29.8).

Crowd Counter & Self Driving RC Car — Robotics

- Used an ESP8266 module to collect WiFi packets released by mobile phones to determine MAC addresses.
- Based upon the number of MAC addresses and a purge mechanism, crowd count is estimated (COVID-19 Application).
- Employed ultrasonic sensors to attain obstacle avoidance and steering in a forward-moving RC car.

Skills

Languages	Python, C++, R, LaTeX, SQL
Tools	Git, Matlab, Spark, LangChain, Pandas, Numpy, Selenium, Matplotlib, Flask, Streamlit, Docker
Cloud Platforms	Google Colab, Amazon SageMaker
ML/DL Frameworks	PyTorch, TensorFlow, scikit-learn, NLTK, HuggingFace
Hardware	Arduino, Raspberry-Pi
Interests	Adversarial ML, Explainability, Computer Vision, Recommendation Systems, LLMs

Certifications

- **Applied Text Mining using Python.** — University of Michigan
- **Applied Machine Learning using Python.** — University of Michigan
- **Introduction to Data Science in Python.** — University of Michigan
- **Convolutional Neural Networks in TensorFlow.** — Coursera
- **Natural Language Processing in TensorFlow.** — Coursera
- **Improving Deep Neural Networks: Hyperparameter Tuning, Regularization & Optimization.** — Coursera
- **Introduction to Tensorflow for Artificial Intelligence, Machine Learning & Deep Learning.** — Coursera
- **Neural Networks and Deep Learning** — Coursera

References

Prof. Apurva Narayan
University of British Columbia
University of Waterloo
Email: apurva.narayan@uwaterloo.ca

Prof. Hongliang Ren
Chinese University of Hong Kong
National University of Singapore
Email: Ren@labren.org

Prof. Arun Buduru
Dept. of Computer Science
IIIT-Delhi, India
Email: arunb@iiitd.ac.in

Dr. Lalithkumar Seenivasan
Postdoctoral Research Fellow
Johns Hopkins University
Email: lseeniv1@jh.edu