Sai Prasath Suresh

ss651@gatech.edu — https://saiprasath21.github.io/ — (404)-528-4492

Objective

Github LinkedIn

International student looking for Full time opportunities in Data Science, SDE - Machine Learning, and Applied Science starting May 2024. (Eligible for STEM OPT Extension)

Education

Georgia Institute of Technology — **Atlanta, USA**
MS in Computer Science - Machine Learning; **GPA: 4.0** — August 2022 – May 2024
Courses: Machine Learning, Natural Language Processing, Web Search and Text Mining, Algorithms

Indian Institute Of Technology (IIT) Bhubaneswar — **Bhubaneswar, India**
B.Tech/M.Tech, Computer Science and Engineering; **GPA: 9.79/10** — July 2017 – May 2022
Courses: Data Analytics, Operating Systems, Computer Networks, Database Management Systems

Skills

Programming Language: Python, C, C++, JavaScript, Java, SQL, HTML
Libraries: PyTorch, Tensorflow, Keras, Hugging Face, Pandas, Numpy, Matplotlib, Scikit-Learn, NLTK, Open CV

Work Experience

Computational Data Science Lab (CLAWS) - Student Researcher *Aug'23 - Present*

- Designing defense techniques for improving the adversarial robustness of **BERT, GPT and Llama2 LLMs**.
- Creating a universal classifier that leverages LLM embeddings to **effectively identify and prevent the generation of harmful content**.

Keysight Technologies - Machine Learning R&D Intern *May'23 - Aug'23*

- Enhanced the **ML Testing toolbox** by developing mutual information based feature visualizations and integrating SHAP for multi-class classification models.
- Evaluated the end-to-end development of machine learning models (CNN for 5G Beam Selection, Autoencoder Based Channel Estimator and Equalizer, Error Correction Transformers) using Keysight's AI-testing pipeline.

Singapore University of Technology and Design - Deep Learning Intern *Jan'22 - Apr'22*

- Researched and implemented a novel **semi-supervised GAN** for detecting trojaned DNNs. Enhanced detection capabilities by integrating a **Denoising Autoencoder** for attack agnostic one-class training.
- Achieved state-of-the-art performance **+3% AUC** on computer vision tasks while reducing run-time by **15%**.

Publications

Analysis of Continual Learning Models for Intrusion Detection System - IEEE Access [2022]
Intelligent Intrusion Detection System for Smart Grid Application - CyberSA [2021]

Projects

Domain Specific Finetuning of LLMs *Aug'23 - Dec'23*

- Executed domain-specific fine-tuning of LLMs using **parameter-efficient LoRA techniques on Llama2 models**, successfully developing a **specialized chatbot** utilizing the Lamini Docs dataset.
- Investigated the LLM's ability to comprehend newly introduced knowledge, focusing on evaluating its **reasoning capabilities and identifying instances of hallucinations**.

Graph Augmented Transformers for Sequential Movie Recommedation *Jan'23 - Apr'23*

- Designed a user-movie-attribute knowledge graph, and generated user and movie embedding using the **Relational Graph Convolutional Networks**. Augmented a Transformer based sequential recommendation system with the generated graph embeddings for capturing higher order relations [Code]
- Outperformed existing baselines on handling cold start users and **-2.5% Mean Absolute Error** overall

Anomaly Detection in Multi-Variate Time Series *Sep'21 - Dec'21*

- Implemented a **dual attention** (spatial and temporal) based **LSTM/GRU** models to pre-emptively detect anomalies in a power plant control system [Code] [Paper]
- Minimized costs by reducing the false alarm rates to **0.21%** with a high detection accuracy of **97.8%**