

# Sai Prasath Suresh

✉ ss651@gatech.edu — [🌐 https://saiprasath21.github.io/](https://saiprasath21.github.io/) — 📞 (404)-528-4492

## OBJECTIVE

[🌐 Github](#) [🌐 LinkedIn](#)

International student looking for Fall 2023 Coop in Data Science, Machine Learning, and Artificial Intelligence.  
(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

## TECHNICAL PROFICIENCY

**Programming Language:** Python, C, C++, JavaScript, Java, SQL, HTML

**Libraries:** PyTorch, Tensorflow, Keras, Pandas, Numpy, Matplotlib, Scikit-Learn, NLTK, Open CV

## WORK EXPERIENCE

### IPaT, GeorgiaTech - Graduate Research Assistant

Jan'23 - Present

- Developing an Emergency Management Portal using **Flask and REACT** for detecting and visualizing flooding in Georgia counties. The portal will be used for real-time planning and response. [\[Link\]](#)

### 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]

## KEY PROJECTS

### Graph Augmented Transformers for Sequential Movie Recommendation

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 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%**.

### Multi-Class Attack Classification using Reinforcement Learning

Jan'21 - Apr'21

- Designed and developed a **Double Deep Q Network (DDQN)** for detecting cyber attacks, that can also dynamically adapt to changing attack distributions. [\[Paper\]](#)
- Achieved **+6% accuracy** compared to existing benchmarks on the cloud-based 8Tb ISOT-CID dataset.

### Adversarial Attacks on Intrusion Detection Systems

Jul'20 - Sep'20

- Implemented **black-box ZOO and FGSM** attacks on DL based Intrusion Detection System. Handled system specific constraints: binary features, one-hot encoded variables, preserving attack capabilities. [\[Code\]](#)
- Studied various defense mechanisms including adversarial training, defensive distillation, and denoising autoencoder.