Sai Prasath Suresh

Mobile: (+1)404-528-4492
International student looking for Summer 2023 Internships.
Mail ID: ss651@gatech.edu
Github LinkedIn

Educational Qualifications

Georgia Institute of Technology **Atlanta, USA**
Master of Science in Computer Science *August 2022 – May 2024*
GPA: 4.0/4.0

Indian Institute Of Technology(IIT) Bhubaneswar **Bhubaneswar, India**
Dual Degree(B.Tech + M.Tech), Computer Science and Engineering *July 2017 – May 2022*
CGPA: 9.79/10 (First in a class of 70)

Technical Proficiency

- **Programming Language:** Python, C, C++, Java, SQL
- **Libraries:** Tensorflow, Keras, PyTorch, Pandas, Numpy, Matplotlib, Scikit-Learn, Open CV
- **Coursework:** Machine Learning, Interactive Robot Leanring, Natural Langugage Processing, Web Search and Text Mining, Data Structures and Algorithms, Calculus, Combinatorics, Probability, Statistics, OS, Networks, Compilers

Work Experience

- **Research Intern, Karlsruhe Institute of Technology, Germany** *May'21 - Aug'21*
  Exploiting Vulnerabilities in Deep Neural Networks
  - Analysed the vulnerabilities of Deep Neural Networks(DNN) against **adversarial attacks**: Zeroth Order Optimization(ZOO) and Iterative Fast Gradient Sign Method (FGSM).
  - Investigated various defense mechanisms (denoising autoencoder, adversarial training, and defensive distillation) to improve the robustness.
  - Used **Explainable AI** techniques such as SHAP and PDP plots to understand the behaviour of DNNs.
- **Research Intern, Singapore University of Technology and Design** *May'20 - Jul'20*
  Trojan Neural Network Detection using One Class GANs
  - Developed a **semi-supervised GAN** to detect Trojaned DNN models using their output probability distributions.
  - Worked with auto-encoders and shadow models to create positive and negative data points in a one-class setting.
  - The model is attack-agnostic and achieved state-of-the-art performance for detecting modification, blending and parameter attacks on computer vision tasks.

KEY PROJECTS

- **Covariate Shift detection and Continual Learning for Intrusion Detection** *Aug'20 - Mar'21*
  - Identified the problem of **covariate shift** in the NSL-KDD dataset and proposed a framework to detect the nature and magnitude of the change efficiently. [Full Paper]
  - Extended replay(dark experience replay) and regularization(learning without forgetting) based **continual learning** models from computer vision to intrusion detection tasks to handle changing attack distributions.
- **Attack Classification using Double Deep Q Networks** *Aug'19 - Mar'20*
  - Contributed to the developement of a **variational auto-encoder** aided Double Deep Q Network to perform intrusion detection on the ISOT-CID and the NSL-KDD dataset. [Full Paper]
  - Evaluated the performance of the model on daily changing attack patterns and ability to adapt to day-0 attacks.
- **Anomaly Detection using Multi-Variate Time Series Analysis** *May'19 - Jul'19*
  - Developed a dual attention based **GRU** model for analyzing the multi-variate time series data to detect anomalies.
  - Compared the performance of the model with ML model(**random forests, SVM, XGBoost**) and DNNs.

Extracurricular Activities

- **Assistant Coordinator:** Counselling Service Team (2020-21); Lead a team of 50 students for mentoring freshmen.
- **Founding Member:** Academic Council (2021-22); Help students develop relevant tech/soft skills for job placements.
- **Secretary:** of the Literary Society, Students' Gymkhana (2018-19)