

SIDHANT NARULA

+1 (469)560-0078 ✉ sidhantnarula42@gmail.com  [linkedin.com/in/sidhant-narula](https://www.linkedin.com/in/sidhant-narula)

Education

Old Dominion University, VA, USA

PhD in Computer Science (AI Security, LLM Security)

2024 – Present

GPA: 4.0/4.0

Thapar Institute of Engineering and Technology

Bachelor of Engineering in Electronics and Computer

2019 – 2023

Punjab, India

Experience

Old Dominion University

AI Graduate Researcher

2024 – Present

VA, USA

- Worked on a project aiming to capture the entire adversarial space as a “network of thought,” modeling multi-turn jailbreak attempts on LLMs. Leveraged a sandbox simulator to prune and refine potential attacks before launching real, targeted jailbreaks against cutting-edge models. [Skills: Adversarial Attacks, LLM Security]
- Implemented Retrieval-Augmented Generation (RAG) pipelines with LlamaIndex, demonstrating distributed training and integration with LLaMA. [Skills: RAG, LLaMA, Distributed Training, LLMs, Shell]
- Explored prompt engineering techniques—including few-shot and chain-of-thought—to build and refine a practical LLM application. [Skills: Prompt Engineering, Prompt Tuning]
- Developed a document processing system using Azure AI and ML services to extract, classify, and analyze content, providing actionable insights. [Skills: Azure, Git, NumPy, R&D, GitHub]

HSBC

Software Engineer

Jul 2023 – Dec 2023

Pune, India

- Designed and implemented REST APIs to support various front-end functionalities, ensuring robust and secure data exchange between client and server applications.
- Developed and maintained microservices using Spring Boot, enhancing the scalability and performance of the overall application architecture.
- Created machine learning algorithms to accurately forecast bond prices, utilizing Python and relevant libraries such as TensorFlow and scikit-learn, contributing to more informed financial decision-making.
- Worked on LoanIQ, a comprehensive loan management system, where I developed and optimized modules to streamline loan processing and improve user experience.

Nucleus Software

Software Development Intern

Jan 2023 – Jun 2023

Noida, India

- Collaborated on a SAML Single Sign-On (SSO) project, implementing a robust and secure authentication and authorization framework.
- Developed RESTful APIs to enhance data exchange and integration between different systems, improving overall efficiency and data consistency.
- Created dynamic and visually appealing webpages using HTML, CSS, and JavaScript. Leveraged cutting-edge libraries and frameworks such as React.js to build interactive user interfaces.

University Of Georgia, USA

Summer Intern

June 2022 – August 2022

GA, USA

- Developed RNA binding site prediction algorithm using a Deep Learning Model and tested it.
- Attended training sessions of Sapelo2 - high performance computing cluster and processed Big Data.
- Established LISE web server for predicting small molecule binding sites on protein.
- Explored ways to visualize and send a daily report of test results to team members and presented in weekly meetings.

Technical Skills

Languages: C,C++, Python, JAVA, SQL, OOPS Concepts, HTML/CSS, JavaScript

Libraries: Tensorflow, Keras, Pandas, Numpy, Scikit Learn, Scipy, Matplotlib, C++ Stl.

Developer Tools: Eclipse, IntelliJ, Jupyter, Google Colab, Visual Studio, GitHub, Git

Relevant Coursework

Deep Learning • Algorithms Analysis • AI Security • Natural Language Processing