Nikhil Reddy Billa

(826) 240-7311 nikilr@vt.edu
github linkedin scholar webpage

Education

Virginia Polytechnic Institute and State University, Blacksburg Aug 2024 – May 2026
MS in Computer Engineering *3.5/4.0*

National Institute of Technology (NIT), Rourkela July 2018 - June 2022
Bachelor of Technology in Electrical Engineering

Relevant Coursework: NLP, Deep Reinforcement learning, Advanced Machine Learning, Computer Vision, Database Management Systems, Soft Computing Techniques

Focus and Strength

My research focus is committed to innovation in AI aligning with **privacy and safety**, covering memorization in LLMs, adversarial robustness, trustworthiness, and ensuring safety in autonomous navigation.I am seeking a position that aligns with my strengths, enabling me to drive impactful solutions in AI.

Skills

Languages: Python, C++, C#, Matlab
Tools: Git, Jupyter, kubernetes
Frameworks: Pytorch, vLLM, fastai, Spark, MapReduce
Other: LLMs, Computer Vision, Machine Learning, Software Engineering, OOPS, DBMS,Streamlit, SQL

Work Experience

Graduate Research Assistant | *REDS Lab, Virginia Tech* Oct 2024 – Present
Advisor :Dr.Rouxi Jia

- Participating as **Blue team** in the **Amazon Trusted AI Challenge**, **developing Large Language Model**s (LLMs) fo**r generating secure, efficient, and trustworthy code**.
- Optimized LLMs for robust code generation using advanced prompting and developed evaluation pipelines for reliability, security, and performance.
- Implemented **attack models** to generate **malicious and vulnerability injections in code**, analyzing LLMs' susceptibility to adversarial inputs.
- Conducted research on **training data memorization in LLMs**, focusing on the risks associated with extracting private information.
- Developed mitigation strategies to address privacy concerns, enhancing the security and ethical deployment of LLMs.

Software Engineer 1 | *NCR Corporation - Hyderabad, India* July 2022 – Aug 2024

- Developed a next-gen POS system using **Kubernetes** & .NET, improving deployment efficiency and microservice management.
- Integrated **ML-driven anomaly detection i**nto the logging system, **reducing system downtime by 40%** by proactively identifying performance bottlenecks.
- Resolved customer issues, fixed bugs, and conducted code reviews to ensure high quality and maintainability.
- Created an **automation tool** that **reduced log analysis time by 90%,** improving efficiency and eliminating human errors.
- Improved system reliability with Kubernetes orchestration, enabling easy scaling, and modular service updates.

Research Assistant | *ML Lab, International Institute of Information Technology Hyderabad, India* Feb 2022 – July 2023
Advisor :Dr.Girish Varma

- Aimed at improving the **robustness of semantic segmentation** models under **adverse weather conditions** such as rain, fog, and low light.
- Designed a novel **safety metric** to evaluate the performance of segmentation models in autonomous driving scenarios, focusing on **safety and reliability** in adverse weather.
- Developed an AI-based system utilizing OCT scans to accurately **grade arrested retinal development**.
- Used data from different centers and OCT manufacturers and ensured the **system's robustness to device variations** through the implementation of **domain adaptation** techniques

Computer Vision Intern | *KoiReader Technologies - Bengaluru, India* Mar 2021 - June 2021

- Developed a **document classification** system using **LayoutLM**, customizing it for specific business need
- Preprocessed raw documents and **created a custom dataset** for model training.
- Trained **LayoutLM models on custom datasets**, improving document classification accuracy by leveraging deep learning and NLP techniques.

Research Assistant | *Intelligent Systems Lab, NIT - Rourkela, India* Mar 2021 - Jan 2022
Advisor :Dr.Manish Okade

- Introduced a fully end-to-end CNN architecture featuring a **preprocessing layer with high-pass filters** to suppress image content effectively.
- This approach significantly **enhanced the estimation of resize factors** for double-compressed resized images.
- The **proposed network** is fully end-to-end and **does not rely on any hand-crafting.**

Publications & Reviewing

- **Reviewer**, Journal of Information Security and Applications (Elsevier), 2024 – Present.

- F. Shaik, A. Reddy, N.R. Billa , G. Varma, et al.."IDDAW: A Benchmark for Safe and Robust Segmentation of Drive Scenes in Unstructured Traffic and Adverse Weather", **IEEE/CVF Winter Conference on Applications of Computer Vision (WACV) 2024.**

- N.R. Billa, B.P. Das, M. Biswal, M. Okade, "CNN based Image Resizing Forensics for Double Compressed JPEG Images", **Journal of Information Security and Applications**, Volume 81, March 2024, 103693.

- N.R. Billa, Zanhan Tu et al. "International Multi-centre Validation of Unsupervised Domain Adaptation for Precise Discrimination between Normal and Abnormal Retinal Development"

Positions, Activities and Awards

- **Amazon Trusted AI Challenge 2024**: Finalist, innovative solutions in **secure** and **safe code generation**.
- **Technical Lead, ML4E Club**: Led AI-driven initiatives, mentored students in ML research.