SURAJ PATEL MUTHE GOWDA

muthegowda.s@northeastern.edu | (857) 351 9538 | LinkedIn | Portfolio | Boston, MA |

EDUCATION

Northeastern University, Boston, MA [CGPA 4.0] **Expected Sep '26**
Master's in Electrical and Computer Engineering (Computer Vision, Machine Learning and Algorithms)
Relevant Coursework: Computer Architecture, Fundamentals of Computer Engineering, Robotics, Sensing and Navigation, LLM Based Chat Agent

PES University, Bengaluru, India [CGPA 3.8] **May '22**
Bachelor's in Electrical and Electronics Engineering (Embedded Systems)
Relevant Coursework: Digital Signals Processing, Artificial Neural Networks, Data Structures and Algorithms, Soft Computing Techniques, Digital Electronics, Analog Electronics, Microsystems

TECHNICAL SKILLS

Programming Languages:	Python, Java, Kotlin, C, C++, Go Lang, MATLAB
ML/AI Frameworks:	TensorFlow, PyTorch, Hugging Face, OpenCV, LangChain, CUDA, OpenMP
Cybersecurity and Networking:	API Design, Mobile Threat Detection, Phishing and Vishing Protection
Development Tools:	Git, gdb, Valgrind, perf, Debuggers, Profiling Tools
H/W Development and Design:	VHDL, VLSI, Embedded C, Arduino, PCB Design, Shaders, OpenMP

WORK EXPERIENCE

Samsung Research and Development Institute, Bengaluru, India **Apr - Aug '24**
Senior Machine Learning Engineer

- **Engineered a multi-modality threat detection system** that identified 10k+ threats daily, boosting device security by 25% with AI-driven anomaly detection across communication channels
- **Developed and deployed On-Device vishing protection solutions** for Samsung, reducing fraud risk by 40% through real-time machine learning analysis of call patterns, processing up to 100k calls daily
- **Developed a deepfake detection** solution with 92% accuracy using EfficientNet for image analysis and BERT for content detection, reducing identity theft and misinformation by 30%

Samsung Research and Development Institute, Bengaluru, India **Aug '22 - Mar '24**
Machine Learning Engineer

- **Developed mobile security solutions for Knox AI B2B projects** to protect enterprise users from emerging threats, utilizing AI-driven protocols for robust protection
- **Optimized AI security models** to enhance user security by improving threat detection accuracy by 20% through fine-tuning with real-world data to detect and mitigate vulnerabilities in enterprise devices
- **Implemented bootloader-level security features on Exynos and Qualcomm chipsets** to ensure secure device startup and protect sensitive user data from unauthorized access
- **Integrated DevOps tools for automated data generation** and analytics, reducing security update deployment time by 35% and enabling real-time protection for 500k+ users, while enhancing system efficiency in threat detection and mitigation

Samsung Research and Development Institute, Bengaluru, India **Jan - Jul '22**
Student Intern

- **Engineered inter-process communication between shaders** to enhance data transfer and processing, boosting rendering performance while utilizing Shader Storage Buffer Objects
- **Developed various shaders (Fragment, Vertex, Compute, and Geometric)** using OpenGL and Vulkan, improving rendering quality in Android projects built with Android Studio
- Implemented parallel computing techniques for GPU based acceleration in real time applications

ACADEMIC PROJECTS

Optimization of Cache Management Using AI **Sep - Dec '24**

- Developed AI-driven cache management strategies using **supervised learning algorithms** to predict cache hit/miss patterns, improving memory access efficiency and minimizing processor stalls to enhance performance in high computing environments
- Applied **reinforcement learning** algorithms to dynamically adjust cache policies based on real-time feedback, leveraging Valgrind and Cachegrind tools to track access patterns, benchmark AI-driven policies against traditional ones, and achieve improvements in energy efficiency and system latency

PUBLICATIONS

Multimodal Strategy to Defend Mobile Devices Against Vishing Attacks, ACM MobiCom '24, Link **Dec '24**
A Multimodal Vishing Threat Detection (MmVTD) framework, which leverages transformer encoders across multiple data modalities such as call transcripts, mobile screenshots, and OCR-extracted text, to detect Vishing attempts.