Jugal Gajjar

MS in Computer Science, The George Washington University
jugal.gajjar@gwu.edu | +1 (571) 629-4206 | github.com/JugalGajjar | linkedin.com/in/jugal-gajjar | Google Scholar

RESEARCH INTERESTS

Intelligent Autonomous Systems, Large Language Models, Natural and Programming Language Analysis, Anomaly Detection, Agentic AI, Human-AI Interaction, Explainable AI

EDUCATION

MS in Computer Science (Machine Intelligence and Cognition)
The George Washington University, *Washington, DC* May 2026
GPA: 3.95/4.0
Thesis: "AI That Detects, Exploits & Fixes: Autonomous Vulnerability Detection and Remediation"
Advisor: Prof. Shi Feng

B.Tech. in Computer Science and Engineering
Navrachana University, *Vadodara, India* May 2024
CGPA: 9.39/10

PUBLICATIONS

SecureFixAgent: A Hybrid LLM Agent for Automated Python Static Vulnerability Repair
2025 International Conference on Machine Learning and Applications (ICMLA) Dec. 2025

MalCodeAI: Autonomous Vulnerability Detection and Remediation via Language Agnostic Code Reasoning
IEEE 26th International Conference on Information Reuse and Integration (IRI 2025) Aug. 2025

Multimodal Sentiment Analysis on CMU-MOSEI Dataset using Transformer-based Models
arXiv preprint (cs.CL) May 2025

Building Trust: The Sentient AI Framework for Emotionally Intelligent AI
International Journal of Creative Research Thoughts (IJCRT) Nov. 2024

RESEARCH PROJECTS

SecureFixAgent: Hybrid LLM Agents for Vulnerability Detection May 2025 – Aug. 2025
- Developed a hybrid LLM-agentic framework integrated with Bandit for iterative vulnerability detection, patching, and re-validation.
- Fine-tuned open-source models with LoRA on Apple MLX & NVIDIA CUDA, achieving 13.5% higher patch accuracy and 10.8% fewer false positives than baselines.
- Under review at the IEEE ICMLA 2025, with strong potential for acceptance.

VulnGraph: Graph+LLM Embeddings for Vulnerability Detection Jul. 2025 – Sep. 2025
- Engineered a multimodal fusion model combining AST/CFG graph embeddings with LLM semantic embeddings using the proposed two-way gating mechanism.
- Achieved 93.57% accuracy, outperforming GNN-only (+8.36%) and LLM-only (+17.81%) baselines, while producing interpretable saliency subgraphs and natural language explanations.
- Under review at the Complex Networks 2025 Conference (Springer SCI Series, SCOPUS-indexed).

MalCodeAI: AI-Powered Malicious Code Detection Jan. 2025 – May 2025
- Designed a dual-stage LLM pipeline using fine-tuned Qwen2.5-Coder-3B-Instruct for semantic code understanding and vulnerability detection and remediation suggestion.
- Integrated exploit reasoning, CVE scoring, and automated patch generation.
- Inspired ongoing thesis work and published and presented at the IEEE IRI Conference 2025.

Multimodal Sentiment Analysis using Transformers Mar. 2025 – May 2025.
- Utilized transformer-based early fusion on the CMU-MOSEI dataset for multimodal sentiment analysis.
- Achieved 97.87% 7-class accuracy and a 0.9682 F1-score by integrating text, audio, and visual modalities.
- Published the preprint on arXiv (cs.CL).

EzyCart: Computer Vision Powered E-Cart System Jul. 2023 – May 2024
- Engineered a patent-pending embedded system using real-time computer vision for autonomous object detection and pricing.
- Trained and deployed lightweight CV models (YOLOv5) on edge devices for efficient and low-latency inferencing with more than 95% accuracy.
- Demonstrated applied skills in CV, embedded ML, and hardware-software integration.

RELEVANT EXPERIENCE

Graduate Assistant
The George Washington University, *Washington, DC* Sep. 2025 – Present
- Supporting an upper undergrad- & graduate-level Big Data and Analytics course (CSCI 4907/6444).
- Guiding students on assignments and projects, focusing on tools like Hadoop and S3 Bucket, and programming in languages like Python, Java, and Linux-Bash.
- Assisting with analytical methods, including machine learning, and provided support for cloud-based and distributed systems projects.

Independent Researcher
The George Washington University, *Washington, DC* Jun. 2025 – Present
- Conducting thesis research on autonomous AI systems for vulnerability detection, exploitation, and remediation in software.
- Designing a secure code analysis pipeline using LLMs, reasoning models, and agent-based simulation architectures.
- Exploring exploit generation and patching strategies using dynamic analysis techniques.

Teaching Assistant
Navrachana University, *Vadodara, India* Jan. 2025 – May 2025
- Mentored 80+ undergraduate students through code review, grading, and structured feedback on 750+ lab reports.
- Assisted in designing rubrics, evaluating technical writing, and improving student understanding of test-driven development.
- Supported curriculum delivery in collaboration with faculty, focusing on code quality, documentation, and debugging.

NVIDIA Jetson AI Project Coordinator
Navrachana University, *Vadodara, India* Mar. 2022 – Jun. 2022
- Conducted workshops on CV and NLP using the Jetson Nano platform, introducing students to embedded AI and real-time inference.
- Mentored 5+ student research projects selected by the NVIDIA Deep Learning Institute.
- Promoted student research initiatives and hands-on learning in edge AI systems.

SELECTED TECHNICAL PROJECTS

SciChat: PDF-Aware Contextual LLM Interface
- Built a domain-adaptive LLM using Mistral7b, Ollama, LangChain, and Pinecone to provide grounded responses over scientific PDFs.
- Showcases toolchain integration, retrieval-augmented generation (RAG), and prompt engineering.

Crypt Chat: Secure Android Messenger with AES-256 & Steganography
- Designed a privacy-preserving mobile chat app employing AES-256 encryption and LSB image steganography for covert message transmission.
- Demonstrates understanding of secure communication protocols and applied cryptography.

CERTIFICATIONS & HONORS

GW SEAS Dean's Award Scholarship	2024
Runner-Up, Tinkerthon 2.0 Hackathon	2023
NVIDIA Jetson AI Specialist	2022
Gold Medalist, International Karate Championship (Team India)	2019

SKILLS

Languages: Python, Java, C/C++, SQL, MATLAB, JavaScript, HTML/CSS
Frameworks: TensorFlow, PyTorch, Scikit-learn, LangChain, LlamaIndex, HF Transformers
Tools: Git, Flask, OpenCV, Pydantic, Tableau, Ollama, Pinecone, Apple MLX, Unsloth AI, W&B, OpenAI API, Gemini, Spark, Docker, Wireshark, BurpSuite, Nmap, Zotero, Rayyan, Elicit
Areas: AI/ML, LLMs, Cyber Security, Deep Learning, Computer Vision, NLP, Software Engineering