

Nicole Villavicencio-Garduño

nicolevill@icloud.com | (205) 544-4164 | www.nicolevgarduno.com

EDUCATION

Carnegie Mellon University

Pittsburgh, PA

Master's in Information Security, focus in AI Engineering — December 2025

Birmingham-Southern College

Birmingham, AL

Bachelor of Honors in Computer Science, concentration in Software Engineering — May 2024

TECHNICAL SKILLS

Programming/Systems: Python, Bash, Linux

AI/ML: Computer vision, CI/CD pipelines, data preprocessing, RAG/MCP/DSPy, feature engineering, evaluation

Infrastructure: Docker, Hadoop/MapReduce, Google Kubernetes Engine (GKE), Google Cloud

RELEVANT WORK EXPERIENCE

Los Alamos National Laboratory

Los Alamos, New Mexico

Adversarial AI Post-Master's Researcher

May 2025 - Present

- ML lead for developing a multi-agent orchestration system for automating end-to-end ML workflows.
- Building preprocessing pipeline for classifying acoustic signal data using XGBoost, Optuna, and Python.
- Presenting technical findings to senior stakeholders through written reports and briefings.

Blue Cross and Blue Shield of Alabama

Birmingham, AL

Technology Support Intern

May 2024 - August 2024

- Rotated through IT teams; mainframe operations, help desk, workstation support, procurement, and asset management to build foundational exposure to enterprise IT operations.

Southern Research

Birmingham, AL

Cybersecurity Analyst

Sept. 2023 - May 2024

- Monitored Microsoft Azure security alerts to identify phishing-affected employees; investigated incident history, coordinated remediation, and applied vulnerability patches across endpoint devices.
- Wiped, reimaged, and reconfigured Windows workstations for redeployment (BitLocker key regeneration).
- Audited company's physical device inventory against tracking-system.

PROJECTS

Giving AI a Headache: Acoustic Adversarial Attacks on Computer Vision

- First-authored paper ([SPIE 2026](#); [arXiv:2606.14658](#)), demonstrating how acoustic attacks degrade YOLOv11 object detection by acoustically resonating camera hardware.
- Designed and ran physical experiments generating acoustic waveforms and recorded live footage of attacks against COCO dataset to measure impact on computer vision model's performance.
- Demonstrated attack evades traditional defenses causing a ~10% drop in detection rate and >7% drop in model confidence.

StayAwake: Real-time Drowsiness/Attention Detector

- Built real-time computer vision tool detecting eye closure, yawning, and user distraction.
- Designed individual-specific calibration methodology: allowing tool to be used across any user.
- Achieved a 91% accuracy for eye-closure, 88% accuracy for yawn detection, and 83% accuracy for distraction detector. Validated each against labeled ground truth per-frame measurements.

GoNoGo: Automated Quality-Gated Pipeline for Big-Data Workflows

- Built pipeline to orchestrate a Hadoop MapReduce job only when the SonarQube quality gate passes, preventing low-quality code from consuming compute on the downstream big-data job.
- Architected and deployed CI/CD pipeline across three GKE clusters provisioned via Terraform, where Jenkins triggers automatically on every Git commit and runs SonarQube static analysis inside Docker before anything downstream executes.