
EDUCATION

The University of Texas at Austin

Austin, TX

*B.S. in Computational Engineering, Cockrell School of Engineering**Expected May 2030*

- **Program:** First undergraduate computational engineering program in the U.S. — numerical methods, scientific computing, and simulation within the Department of Aerospace Engineering and Engineering Mechanics

WORK EXPERIENCE

CoGuide (coguide.ai)

Austin, TX / Irving, TX / San Francisco, CA

*Founding Engineer / Member of Technical Staff**Jan 2026 – Present*

- Build systems for an AI instructional-insight platform that turns real classroom audio into private coaching feedback for teachers and aggregate engagement trends for schools.
- Designed and built the entire production backend in Rust (~30k-line codebase, closed source) and stood up the full AWS infrastructure, scaling the platform from zero product to deployments in 10+ schools.
- Engineered the audio transcription and speaker-diarization pipeline with custom CUDA fusion kernels and VAD-based batching on legacy NVIDIA T4 GPUs — 2x the cost efficiency of market alternatives and 10x that of AWS Transcribe.
- Engineered a two-stage computer-vision pipeline (YOLOv8 person detection + upper-body pose estimation) detecting hand-raise engagement events in classroom video at ~0.96x real-time on GPU, emitting annotated video and timestamped JSON/NDJSON event logs — open-source miniproject; production work is closed source.

PUBLICATIONS

• Rule-based Tensor Mutations Embedded within LLMs for Low-Cost Mathematical Computation:

Ayyalasomayajula, S. (2025). TechRxiv preprint (IEEE). Sole-authored architecture embedding deterministic, GPU-optimized fixed-index tensor-mutation modules inside transformer LLMs (LLaMA 3B) for low-latency, step-wise-exact arithmetic and linear algebra — improving mathematical-reasoning benchmarks without retraining or external symbolic engines. doi:10.36227/techrxiv.175393256.68603080/v1

PROJECTS

- **exalock — GPU-First Wayland Lockscreen** (WIP, source): Building a from-scratch, zero-toolkit lockscreen for Hyprland/Wayland in C/C++23 and GLSL, speaking raw Wayland protocols (`ext-session-lock-v1`) with per-output lock surfaces, EGL contexts, and a frame-callback-driven OpenGL ES render loop. Engineered a GPU “silk” particle simulation from first principles: divergence-free stream-function velocity fields integrated with RK4 and vorticity-based color mapping. PAM authentication and hardening are in active development.
- **Real-Time Quantitative Analysis Streamer** (closed source): Independently engineered a high-frequency financial data ingestion and analysis platform for a family quant team, sustaining **100K datapoints/s** via Kafka, Mosquitto MQTT, and DXLink streaming. Integrated Tastytrade APIs and Paho clients with a ClickHouse backend for low-latency tick storage and real-time analytics. Developed C++ computational modules executing LSTM-driven predictive models alongside live Heston and Black-Scholes pricing for SPX, NDX, and derivative instruments, with Grafana dashboards for latency, spread, and volatility observability.
- **MQTT-to-Push Notification Pipeline** (C++ · Rust · RSS): Architected a three-service notification backbone ingesting MQTT5 messages and delivering mobile push via `ntfy.sh`. Benchmarked head-to-head C++ (Paho) and Rust (`rumqttr/tokio`) consumers, with the async Rust rewrite sustaining **10M notifications/s** at 1KB payloads and adding tap-to-open link actions. Built the Python RSS producer with MD5-hash deduplication and QoS-1 MQTT publishing; the pipeline has relayed **10k+** real-time news alerts to devices since August 2025.
- **Matrix FS** (closed source): Developed a Layer 2 distributed storage protocol atop IPFS in Rust with a Tauri/Svelte frontend. Engineered end-to-end encrypted file sharing with AES-256-CBC and ChaCha20-Poly1305 AEAD, deterministic content-addressing tokens, MIME-aware retrieval, and SurrealDB ticketing over Tor hidden services for privacy-preserving access control and auditability.
- **Home Infrastructure and OSS Deployment:** Designed, implemented, and maintain self-hosted infrastructure supporting 50 concurrent users with partial monetization. Operate three high-availability servers and 40+ Docker containers across mail (Postfix/Dovecot), LangChain/LangFlow NLP workflows, n8n automation, RTP streaming, WireGuard mesh networking, and static/dynamic web services. Built custom tooling for routing, 150TB ZFS-backed NAS storage, container orchestration, and zero-trust secure access gateways.

- **CyberPatriot Automation Scripts for USAF**: Developed a comprehensive suite of proprietary automation scripts in Rust and PowerShell for vulnerability remediation/hardening automation for USAF CyberPatriot teams. The Unix-based scripts consistently contributed over 30 points per competition round by rapidly identifying and mitigating security flaws on Linux/Unix targets with sub-2-minute execution times. Windows counterparts, built in PowerShell, achieved over 25 points regularly. The toolkit was later licensed and transferred to another CyberPatriot team for ongoing development and competitive use.
- **Browser-Security Red-Team PoC** (educational; source): Built, in under 12 hours, a TypeScript/Bun + Playwright proof of concept demonstrating how stealth-patched headless browsers defeat commercial bot detection: `dom.webdriver` suppression, fingerprint-evasion plugins, and authenticated session-state reuse driving fully automated crawling and interaction on a major professional network. Documents concrete gaps in client-side bot defenses; for educational purposes only.
- **Hardened SSH Portfolio Server — Security PoC**: Deliberately exposed a self-built stack — native C++ FTXUI terminal UI over SSH (`ssh krishna@krishna.ayyalasomayajula.net`) plus a Next.js/Tailwind front end — on a bare-metal production server with full home-LAN access, as a live proof of concept of my code and system hardening. Survived **1M+ automated attacks from 100 countries** over 18 months of continuous operation with zero compromise.

INVOLVEMENT

- **Research Assistant to Dr. Madan M. T. Ayyalasomayajula (2022–Present)**: Supporting literature review, tooling evaluation, and benchmarking for ongoing ML research.
- **President, Cybersecurity Club at PESH (2023–2026)**: Led hands-on workshops on ethical hacking, CTF preparation, and digital forensics; mentored students on Linux fundamentals, reconnaissance, and safe operational practices.
- **Trace Labs OSINT Search Party (2023–2024)**: Contributed to missing-person investigations using open-source intelligence, including pivoting, breach-data analysis, geolocation, and metadata extraction.

HONORS & AWARDS

- **Lockheed Martin Cyber Quest — 2nd Place (2025)**: Placed second among approximately a hundred competitors in the DFW metroplex; served as team captain and earned 30% of team score.
- **CyberPatriot — State Level Gold Tier (2025)**: Led offensive security analysis in a blue-team environment, applying red team techniques to test team defense resilience.
- **NSA Codebreaker Challenge — November 2024**: Solved 5 tasks involving real-world cyber scenarios including protocol exploitation, red team tooling, and reverse engineering.
- **National Merit Commendation — PSAT 2024–2025 Scholastic Year**: Ranked within the top 50,000 NMSQT PSAT scorers.
- **Hack The Box (HTB)**: Completed 15+ medium machines, peak global rank 564.

SKILLS

Languages: Rust (async/unsafe/FFI), C, C++ (23), Python, TypeScript, Java, Bash, SQL, GLSL

Systems & Infrastructure: Linux (Arch/Debian/Proxmox), Docker/Podman (40+ containers, HA), WireGuard, Nginx/Traefik, PostgreSQL, ClickHouse, Redis, Kafka, MQTT, gRPC, ZFS (150TB+), zero-trust networking

Scientific Computing: NumPy/SciPy/JAX, Eigen, BLAS/LAPACK, CUDA/cuBLAS, ODE solvers (RK4/RK45), optimization (cvxpy), PyTorch

Security: reverse engineering, binary exploitation, network forensics, hardening/sandboxing (eBPF, seccomp, AppArmor), red/blue-team tooling (nmap, Burp Suite, Metasploit, Wireshark, hashcat)

Frontend & Embedded: Next.js/React, Svelte, Tauri, FTXUI, STM32/ESP32, cross-compilation