krishna@ayyalasomayajula.net
(214) 293-5743

Krishna Ayyalasomayajula

https://krishna.ayyalasomayajula.net
US Green Card Holder

Education

Plano East Senior High School — Plano, TX
Multi-disciplinary & STEM endorsement — *Aug 2022 – Aug 2026*

- **Concentrations**: Computer Science & Mathematics
- **Coursework**: Data Structures & Algorithms, Object-Oriented Programming, Calculus, Differential Equations, Probability, Statistics, Newtonian Physics

Projects

- **Preprint: Rule-based Tensor Mutations Embedded within LLMs for Low-Cost Mathematical Computation**: Authored a novel architecture enhancement embedding deterministic tensor mutation modules within transformer-based LLMs (LLaMA 3B) to enable low-latency, step-wise accurate arithmetic and linear algebra computation. Leveraged GPU-optimized fixed-index tensor operations to circumvent probabilistic inference bottlenecks, achieving substantial improvements in mathematical reasoning benchmarks without retraining or external symbolic engines. Published on TechRxiv.
- **MQTT–to–Push Notification Pipeline**: Developed a 3-repository system to ingest MQTT5 messages and forward them as mobile push notifications via `ntfy`. Benchmarked ingestion libraries in both C++ and Rust, with Rust outperforming at **10M notifications/s** (1 KB each). Deployed a Python-based deduplicating ingest service using hash sets, which has successfully relayed 10k+ real-time news alerts to devices in the August of 2025. Designed for scalability, throughput, and reliability in high-volume messaging.
- **Matrix FS**: Developed a Layer 2 distributed storage protocol atop IPFS, implemented in Rust with a performant Tauri-based Svelte frontend. Engineered end-to-end encrypted file sharing using AES-256-CBC and ChaCha20-Poly1305 AEAD schemes with deterministic tokenization for content addressing. Extended IPFS functionality with MIME type encoding to enable file-type-aware decentralized storage and retrieval. Integrated SurrealDB ticketing over Tor hidden services to facilitate privacy-preserving access control and auditability.
- **Bon Voyage (MLH Hackathon Project)**: Designed and implemented an AI-powered MOOC content generator leveraging Java and Stanford CoreNLP for natural language understanding, annotation, and semantic parsing. Employed advanced NLP pipelines to extract and structure knowledge from raw educational resources, enabling dynamic course syllabus generation and personalized learning paths.
- **2022 Regional Science Fair Project**: Architected an AI-driven personalized learning assistant combining OpenAI API integration and self-hosted GPT-2 models for scalable, context-aware content recommendation. Engineered multi-modal resource retrieval aggregating scientific papers, educational videos, and curated articles with semantic similarity search and relevance ranking for comprehensive knowledge dissemination.
- **Home Infrastructure and OSS Deployment**: Designed, implemented, and maintain a scalable, enterprise-grade self-hosted infrastructure supporting 50 concurrent users with partial monetization. The system architecture includes three high-availability servers orchestrating over 40 Docker containers leveraging microservices for mail servers (Postfix, Dovecot), LangChain and LangFlow NLP automation workflows, n8n event-driven automation, multicast RTP streaming clusters, WireGuard VPN mesh networking, and multiple static/dynamic web services. Contributed upstream patches and custom modules to OSS projects, while developing bespoke tooling for advanced network routing, storage management ($\geq$ 150 TB NAS with ZFS), container orchestration, and secure access gateways following zero-trust principles.
- **SLAM Guide for Autonomous Robotics**: Developed an in-depth technical guide on probabilistic Simultaneous Localization and Mapping (SLAM) grounded in Durrant-Whyte's seminal 2006 survey. Documented key algorithms such as EKF-SLAM, particle filters, and graph-based optimization methods with application insights derived from hands-on F1Tenth robotics platform experience. The guide serves as a resource bridging theory and real-time robotics system implementation.
- **CyberPatriot Automation Scripts for USAF**: Developed a comprehensive suite of proprietary automation scripts in Rust and PowerShell to optimize vulnerability scanning and exploitation tasks 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.

- **SSH-Driven Portfolio Site**: Deployed a web-accessible terminal prompt at krishna.ayyalasomayajula.net, inviting users to connect via `ssh krishna@krishna.ayyalasomayajula.net` for a fully interactive TUI showcase. Designed with Next.js and Tailwind CSS, featuring Aceternity-inspired cursor effects and a cinematic blur aesthetic. The SSH endpoint launches a native C++ FTXUI interface highlighting projects, real-time system status, and personalized Easter eggs, emphasizing a hacker-first, command-line-native identity.

Involvement

- **Research Assistant to Dr. Madan M. T. Ayyalasomayajula (2022–Present)**: Assisted in identifying relevant literature and summarizing key concepts to support ongoing research. Helped explore suitable tools, libraries, and frameworks for implementation tasks. Participated in discussions on research direction and contributed to benchmarking efforts under guidance. Gained experience with evaluating prior work, literature reviews, and understanding technical workflows in a research setting.
- **President, Cybersecurity Club at PESH (2023–2026)**: Led the school's cybersecurity club. Organized hands-on workshops on ethical hacking, CTF prep, and digital forensics. Mentored students on Linux fundamentals, reconnaissance techniques, and safe operational practices.
- **Officer, Computer Science Club at PESH (2023–2026)**: Taught students data structures, algorithms, and practical programming through peer instruction. Led Java instruction sessions, introduced Git workflows, and organized coding challenges.
- **Trace Labs OSINT Search Party (2023–2024)**: Contributed to global missing person investigations using open-source intelligence. Employed pivoting strategies, breach data analysis, geolocation, and metadata extraction to submit actionable reports.
- **IT Army of Ukraine (Dec 2023 – Feb 2024)**: Led a small offensive squad targeting publicly sanctioned scope ranges. Coordinated denial-of-service campaigns, resource enumeration, and persistent takedowns—successfully disabling at least one high-value scope each month in support of Ukraine's digital resistance.

Honors & Awards

- **CyberPatriot — State Level Gold Tier (2025)**: Led offensive security analysis in a blue-team environment. Applied red team techniques to simulate attacks and test team defense resilience.
- **Lockheed Martin Cyber Quest — Second Place (2025)**: Placed second among approximately a hundred competitor in the DFW metroplex. Contributed low-level security logic and reverse engineering skills to the team. Served as team captain, and earned 30% of team score.
- **Hack The Box (HTB)**: Completed 15+ Medium-difficulty machines with a peak global rank of 564. Specialized in red team tactics such as binary exploitation, lateral movement, and privilege escalation. Achieved over 90% progress toward the 'Hacker' rank.
- **TryHackMe — King of the Hill (2024)**: Ranked in the Top 5 on the KoTH leaderboard for two consecutive days. Demonstrated live red team capabilities in adversarial environments.
- **Battle of the Brains — Spring 2024 (Advanced Division)**: Tied for 5th place in a regional algorithms competition. Contributed advanced problem-solving and systems-level strategy under time pressure.
- **Battle of the Brains — Spring 2025 at UTD (Advanced Division)**: Tied for 10th place. Demonstrated proficiency in competitive algorithmic programming and system optimization.
- **NSA Codebreaker Challenge — November 2024**: Solved 5 advanced tasks involving real-world cyber scenarios including protocol exploitation, red team tooling, and reverse engineering.

Skills

Languages: Rust (5/5), Async Rust, Python, Java, Bash/ZSH, C/C++, PowerShell, TypeScript, Solidity, SQL, YAML, TOML, JSON, Protobuf
Networking & Protocols: WireGuard, Tailscale, Yggdrasil, Tor, I2P, I2C/SPI, DNS, DHCP, TLS, HTTP/2, gRPC, QUIC, SCTP, TCP/IP stack analysis, NTP/SNTP fuzzing
Security & Offensive Tooling: Reverse engineering, binary exploitation, ROP, shellcode crafting, steganography, malware analysis, client-auth via ephemeral keys
Red Team Tooling:

- *Recon:* `amass, subfinder, assetfinder, dnsx, httpx, ffuf, waybackurls, gau, hakrawler, katana, shodan, theHarvester`
- *Web Vuln:* `nikto, sqlmap, XSStrike, wfuzz, dalfox, Nuclei, Burp Suite Pro, OWASP ZAP, dirsearch`
- *Post-Exploitation:* `Empire, Covenant, Metasploit, Cobalt Strike, Pupy, Sliver, Ligolo, netexec (CrackMapExec), mimikatz, impacket`

- *Active Directory:* `BloodHound, SharpHound, Rubeus, Kerbrute, ntlmrelayx, secretsdump, ldapsearch, adidnsdump, dcsync`
- *Privilege Escalation:* `linPEAS, winPEAS, pspy, gtfobins, BeRoot, PowerUp, JuicyPotato, Seatbelt`
- *Payloads & C2:* `msfvenom, Unicorn, Veil, Nishang, CS, Covenant, Mythic, Havoc`
- *Exploitation/Scanning:* `nmap, rustscan, masscan, Nessus, OpenVAS, metasploit, searchsploit, exploitdb`
- *WiFi/Bluetooth:* `aircrack-ng, kismet, hcxdumptool, bettercap, hydra`
- *Misc:* `tcpdump, tshark, Wireshark, mitmproxy, socat, responder, evil-winrm, fcrackzip, hashcat, John, nginx`

Big Data & Analytics: TimescaleDB, hypertables, ClickHouse, Apache Kafka, Roaring Bitmaps, Redis Streams, Pinecone, Bloom Filters
Backend/Data Infra: PostgreSQL, SQLite, Redis, MinIO, gRPC, Flatbuffers, REST APIs, custom protocol engineering (binary/streamed), Kafka Connect
Cloud & IaC: AWS (EC2, S3, Lambda, CloudFront, Route 53, IAM, Secrets Manager), Terraform, OCI, Cloud-init, systemd cloud unit orchestration
Linux & Systems: Arch Linux, Debian, kernel patching, cgroups v2, namespaces, FUSE, sandboxing (bubblewrap, Firejail), QEMU/KVM, LXC, systemd, BPF/eBPF, AppArmor, Seccomp
Cryptography: ChaCha20Poly1305, Argon2id, Ed25519, ECDSA, Kyber1024, Dilithium5, AES-GCM, X25519, TLS 1.3, NaCl/Libsodium, custom HMAC/KDF schemes
DevOps & Tooling: Git, GitHub Actions, Make, CMake, Cargo, Docker, Podman, Nix, systemtap, gdb, perf, strace, tmux, jinja2, jq, yq, GNU coreutils