Mahmudul Hasan

Forward Deployed AI Engineer & Senior Systems Architect

Frontier LLM Evaluation (MCP/RLHF) · Reverse Engineering & Red-Teaming · Embedded IoT & Bare-Metal Systems

📍 **Dhaka, Bangladesh** (Full US/EU Overlap) 📧 mahmudul8296@gmail.com 📱 +8801912409071 💻 github.com/bdlogicalerror

🌐 bdlogicalerror.github.io 🔗 linkedin.com/in/bdlogicalerror

> ⚡ **Hardware & Verified Infrastructure:** Apple Silicon MacBook Pro (macOS Sequoia) · Bare-Metal Linux Worker Cluster (30+ Containers) · RP2040 Pico Hardware Lab · ESP32-C3 & ESP8266 IoT Workstation · Studio Audio (GK74 Pro)

EXECUTIVE SUMMARY

Polymathic **Forward Deployed AI Engineer & Senior Systems Architect** with 10+ years of production experience bridging frontier AI models (OpenAI, Anthropic, Google DeepMind, DeepSeek) with enterprise hardware, IoT, and high-concurrency systems. Recognized for deep multi-domain mastery: bridging legacy customer hardware (DVRs, RTSP/ONVIF streams, microcontrollers) to agentic AI pipelines (**Model Context Protocol [MCP]**, vector search, function calling), conducting advanced binary & Android reverse engineering, and executing production IoT firmware (ESP8266/ESP32, RP2040). Power user on Apple Silicon and bare-metal Linux infrastructure supervising distributed Celery task queues, Suricata network IDS/IPS, and `launchd` daemons. Achieved a **100% first-shot pass rate on frontier model benchmarks and technical evaluation deliverables**. Available immediately for Forward Deployed Engineering, AI contributor, and systems architecture contracts.

CORE SPECIALIZATION PILLARS & TECHNICAL MASTERY

1. Frontier AI Model Evaluation & Model Context Protocol (MCP): Frontier Models (GPT-4o, o1, o3-mini, Claude 3.7 Sonnet, Gemini 2.0, DeepSeek R1/V3, Llama 3.3), **Model Context Protocol (MCP)**, Function Calling, Portkey AI Gateway Orchestration, Hybrid RAG (pgvector 384-dim dense + BM25 FTS), SWE-bench Code Verification, RLHF Pairwise Preference Auditing (>85% What/Where/Why Action Density, Strict Anti-Silence Narration).

2. Forward Deployed Engineering (FDE) & Enterprise AI Integration: Turnkey integration bridging legacy enterprise hardware (DVR/NVR video feeds, RTSP/ONVIF streams, sensors) to real-time AI pipelines (DVRify, VeloTrack), edge computer-vision, vector search indexing, asynchronous event dispatching, and automated API-UI contracts.

3. Vulnerability Research, Reverse Engineering & Adversarial AI Red-Teaming: Android APK Bytecode & Smali Reversing (JADX, APKTool, Baksmali), Native Binary (.so) & White-Box Cryptography (Ghidra, IDA, radare2, KonaShield/KonaWbc), Dynamic Instrumentation (Frida hooks), Cryptanalysis (Triple-DES / DESede, AES, salt extraction), 802.11 Layer-2 Frame Injection (raw deauth, beacon floods, evil twin), AI Safety Red-Teaming (TAP, FlipAttack).

4. Embedded Systems, Microcontrollers & IoT (ESP8266, ESP32-C3, RP2040 Pico, LoRa, BLE): Espressif SoCs (ESP8266 lwIP NAPT bridge, ESP32-C3 SuperMini RISC-V), RP2040 Raspberry Pi Pico USB HID Electrical Signal Synthesis (TinyUSB, CircuitPython, Neuromuscular Gaussian Physics), LoRa Sub-GHz RF Framing (SX1278 433MHz, CAD listening loops), Apple Find My BLE (OpenHaystack), Deep-Sleep MPU6050 Interrupt Wake, CoreAudio HAL Darwin Daemons.

5. Systems Programming & High-Level Languages (Rust, Go, Python, C++, Swift, Kotlin, Java, TypeScript): Rust (Tauri v2), **Go / Golang** (high-concurrency networking), **Python** (AsyncIO, FastAPI, PyTorch), **C++** (11/14/17, firmware), **Swift** (iOS native CoreBluetooth/CMMotion), **Kotlin & Java** (Android native foreground services, GATT, JNI), **Dart / Flutter 3.x** (Shorebird 2.0 OTA, Goertzel DSP 10-50Hz), **TypeScript** (React 19, Next.js 15), **PHP / Laravel**, **SQL** (PostgreSQL, pgvector).

6. Distributed Cloud Infrastructure & Bare-Metal Worker Clusters (Docker, Celery, Suricata, go2rtc, pgvector): Bare-Metal Linux Worker Cluster (30+ Docker containers, Celery distributed task queues, Redis, Flower), Suricata Network IDS/IPS, ntopng real-time traffic analysis, go2rtc ultra-low latency WebRTC/RTSP gateway, Cloudflare Zero-Trust Tunnels (cloudflared apex edge ingress without open ports), macOS Machine-Wide Process Governance (launchd SSOT, flap guards).

PROFESSIONAL EXPERIENCE

Senior Forward Deployed AI Engineer & Evaluation Specialist · Frontier AI Research & Evaluation Labs

Jan 2024 – Present | US Remote Contract

- **Frontier Model Evaluation & Benchmarking:** Authored, audited, and benchmarked multi-domain technical tasks spanning **Cybersecurity, Quantitative Finance, Cloud Infrastructure (K8s), and Software Engineering** under strict automated quality criteria.
- **SWE-Bench & Security Red-Teaming:** Conducted granular code auditing and adversarial testing across Python, C++, Go, and TypeScript—detecting API hallucinations, algorithmic race conditions, memory leaks, and prompt injection vectors (TAP/FlipAttack).
- **Ground Truth & CoT Curation:** Authored verified ground truth datasets and complex Chain-of-Thought reasoning trajectories, sustaining >85% cognitive action density (**[Screen Area] + [Window Panel] + [Action Verb] + [Target] + [Purpose]**) with 100% first-pass reviewer approval.
- **Hardware-Level Anti-Detection Automation:** Developed an RP2040 Raspberry Pi Pico USB HID hardware relay with dual-Gaussian typing latency physics (mean 110ms) and cubic Bézier mouse paths, generating authentic electrical `kCGEventSourceStateHIDSystemState` signals that bypass OS synthetic event detection.
- **Reproducible STEM Analytics:** Authored quantitative models with live verified execution—including Credit Default Risk Scoring (ROC-AUC 0.94), SaaS Churn Hazard Modeling ($2.92M ARR portfolio analysis), Kubernetes Pod Resource Optimization, and Supply Chain Analytics.

Staff Systems Engineer & Automation Architect · Slicesoft / US Enterprise Platforms

May 2023 – Aug 2024 | US Remote Contract

- **High-Throughput Microservices:** Architected and maintained distributed backend APIs and automation pipelines in Go, Python, and PHP/Laravel, serving US enterprise platforms with 99.9% uptime.
- **Data Modeling & Vector Optimization:** Designed relational schemas and vector search pipelines (PostgreSQL + **pgvector**), cutting query latency by 45% across multi-million record datasets.
- **Contract-Driven API Integration:** Established OpenAPI/Swagger specifications and contract-driven interfaces bridging frontend React teams and backend data engines with zero contract mismatches.
- **Automated Quality Assurance & CI/CD:** Built Dockerized testing suites (PyTest, Jest) and staging-to-production deployment pipelines, reducing regression rates by 38% and cycle times by 50%.

Full-Stack & Systems Developer · Global Enterprise Remote Contracts — Sep 2022 – Apr 2023 | Remote

- **Scalable Web Platforms:** Delivered full-stack web platforms and administrative portals utilizing React, Node.js, and modern relational databases with strict modular architectures.
- **High-Concurrency Automation:** Developed asynchronous data ingestion pipelines, proxy rotators, and webhook notification services handling thousands of daily events.
- **US Founder Collaboration:** Partnered directly with US founders and engineering directors to translate product roadmaps into verified, production-ready deliverables on schedule.

Senior Frontend & Data Visualization Engineer · C4ADS (Center for Advanced Defense Studies) — May 2017 – Jan 2019 | Washington, D.C. / FL (Remote)

- **Geospatial Intelligence Dashboards:** Built interactive data visualization applications mapping complex global illicit supply chains and multi-node ownership graphs using React, Next.js, Redux, and Mapbox SDK.
- **Performance Profiling:** Optimized large-scale client-side state management and SVG/WebGL rendering, slashing bundle size by 35% and improving LCP/TTI metrics by 50%.
- **Secure Component Design:** Formulated reusable, accessible design systems adhering to strict security protocols for investigative defense researchers.

FEATURED ENGINEERING & PRODUCTION SYSTEMS (ALL 12 PROJECTS COMBINED)

1. DVRify — AI Smart Video Surveillance SaaS & Gateway: Turnkey Forward Deployed AI pipeline transforming any legacy CCTV/DVR/NVR hardware into intelligent surveillance. Ingests RTSP/ONVIF streams via **go2rtc WebRTC gateway**, executing live person/face detection, **PostgreSQL + pgvector** spatial vector search, and automated real-time alert dispatching.

2. VeloTrack & Shikho Mobile Engineering Platforms: Production offline-first vehicle fleet telemetry suite (Flutter 3.x, Dart 3.11, Shorebird 2.0 OTA instant code push, native **Swift CoreBluetooth / Kotlin GATT** bridges, Fastify, PostGIS) with embedded **10-50Hz Goertzel DSP frequency classification** to differentiate engine vibration from pedestrian movement (121 tests); alongside high-scale educational video streaming architecture.

3. Bare-Metal Distributed Worker Node & Ingress Mesh: High-availability bare-metal Linux server cluster hosting 30+ production containers: Celery distributed worker task queues, Redis, Flower monitoring, **Suricata Network IDS/IPS**, Portkey AI Gateway, Model Context Protocol (MCP) servers, and zero-trust Cloudflare edge ingress tunnels.

4. RP2040 Pico USB HID Hardware Stealth Relay: Physical microcontroller synthesizer (RP2040 CircuitPython/TinyUSB) spoofing Apple Magic Keyboard descriptors. Generates electrical D+/D- bus signals with dual-Gaussian typing physics (mean 110ms) and Bézier mouse paths to bypass kernel-level synthetic automation taps.

5. BikeGuard Long-Range IoT & ESP8266 802.11 Pentest/Bridge: Embedded hardware systems: ESP32-C3 SuperMini with 2-10km long-range **LoRa SX1278 (433MHz)** RF alarms, Apple Find My OpenHaystack BLE, and deep-sleep MPU6050 EXT0 wake (0.3-0.5mA); paired with ESP8266 C++ lwIP NAPT network bridge and raw 802.11 management frame injection (deauth, beacon floods, captive portal).

6. apkLab, Android Monitor (amon) & HackAgent AI Red-Teaming: Automated 8-phase reverse engineering pipeline auditing native `.so` boundaries and decomposing Triple-DES (DESede) ciphers; agentless Android ADB remote forensics with RFB/VNC delta streaming; and adversarial AI evaluation gateway executing TAP and FlipAttack jailbreak tests.

EDUCATION, ATTRIBUTES & AVAILABILITY

B.Sc. in Computer Science & Engineering (Applied Systems Practice) · Core Engineering Foundation — 2016 – Present

Core coursework & continuous practice: Systems Architecture, Operating Systems, Cryptography, Embedded Systems, Network Security, Database Systems.

Work Authorization & Availability: Immediate availability for 40+ hrs/week. Full flexibility across US Eastern (EST), Pacific (PST), and European (CET) timezones.

Languages: English (Full Professional Working Proficiency — 10+ years daily collaboration with US engineering teams), Bengali (Native).