

Krish Gupta

Software, Machine Learning & Security Engineer

New Delhi, India | krishgupta3879@gmail.com

[linkedin.com/in/krish-gupta007](https://www.linkedin.com/in/krish-gupta007) | github.com/KrishG7 | leetcode.com/u/KrishGupta0007

Portfolio: krish-gupta.me

SUMMARY

Third-year B.Tech student (Blockchain & Cybersecurity) who builds and tests software end to end: ML model-file security, probabilistic forecasting, clinical AI, Linux system-call tracing and clinic-booking platforms. Python, C, Go and TypeScript; 330+ LeetCode problems; leads teams.

EDUCATION

Faculty of Technology, University of Delhi

New Delhi, India

B.Tech, Computer Science & Engineering (Blockchain & Cybersecurity)

Aug 2024 – May 2028 (Expected)

- **CGPA:** 8.09 / 10.0 (through Semester 2; Semester 3–4 results pending)
- **Relevant Coursework:** Data Structures, Algorithms, Operating Systems, Computer Networks, DBMS, Applied Cryptography, Deep Learning, AI & Machine Learning, Software Engineering

TECHNICAL SKILLS

Languages: Python, C, Go, TypeScript, JavaScript, SQL, Dart, MATLAB, Rust (basic)

ML, Data & Statistics: PyTorch, scikit-learn, XGBoost, pandas, NumPy, SciPy, xarray, YOLOv8, OpenCV, time-series forecasting, NLP (basic: TF-IDF, transformer cross-encoders), retrieval-augmented generation (RAG), knowledge graphs, EMOS, BMA, CRPS, cross-validation

Security: Static analysis, supply-chain security, sandboxing, authentication (JWT, OTP, bcrypt), row-level security, applied cryptography, SARIF

Backend & Systems: Linux, `ptrace`, Docker, AWS, Node.js, Express, FastAPI, Flask, REST APIs, WebSockets, MySQL, PostgreSQL, SQLite

Frontend & Tools: React, Next.js, Flutter, Tailwind CSS, Git, GitHub Actions (CI/CD), pytest, Jest, Vercel

PROJECTS

Aegis-Tensor – ML Model-File Security Scanner | *Python, Rust (PyO3), pytest, SARIF* 2026 – Present

- Lead developer (60 of 80 commits) of an open-source scanner that checks whether an ML model file is safe to load, without loading it: PyTorch pickle, safetensors, GGUF, ONNX and Keras, routed by file signature rather than extension.
- Shipped the security-critical changes: checkpoint-global allowlist, tracking of runtime-built callables, scanning of embedded and legacy-tar storage pickles, and atomic disarm output (no partly disarmed file left behind). The pickle scanner simulates the opcode stack and memo instead of executing code.

WEAVR – Hybrid AI–NWP Rainfall Forecast Blending | *Python, xarray, Zarr, SciPy, EMOS/BMA* SIH 2026

- Smart India Hackathon (SIH) 2026 team project (ATMOSYNC) blending GraphCast with HRES and IFS ensemble forecasts on a 0.25° India grid for 24–96 h monsoon leads; I am a core contributor with 11 merged pull requests on the statistical core and evaluation.
- Built quantile-mapping and Generalized Pareto (GPD) tail-repair modules, spliced continuously into the EMOS forecast distribution; false-zero probability cells at the extreme thresholds fell from 193 to 0.

Athena – AI Cancer Second-Opinion Copilot | *Python, FastAPI, FalkorDB, React, Docker* SIH 2026

- Smart India Hackathon (SIH) 2026 team project: oncology second-opinion engine that answers from a CIViC/PubMed knowledge graph (FalkorDB) with citation-traceable evidence, and keeps patient-case memory in PostgreSQL to flag which earlier findings new results invalidate.

SysCV – Linux System Call Visualizer | *Go, Linux ptrace, Docker, WebSockets, React Flow* 2026

- Browser tool that compiles a C program, runs it under `ptrace` inside a sandboxed Docker container and steps through every system call with arguments, return values and a live kernel graph.

Wait Zero – Smart Clinic Booking | *Node.js, Express, MySQL, React, Flutter, SQLite* 2026

- Lead developer and architect of a six-person course project: clinic booking with a live token queue, emergency (RED) interrupts, GPS geofence check-in and digital prescriptions.

Brahm-Kosh – Codebase Intelligence Engine | *Python (AST), Three.js, WebGL, pytest* 2026

- Offline code analyser that parses 13 languages (true AST for Python, curated adapters for the other 12) into one project/module/file/symbol model; deterministic, no LLM calls.

LEADERSHIP & ACHIEVEMENTS

Competitive Programming: 330+ problems solved on [LeetCode](https://leetcode.com) (142 Easy, 151 Medium, 40 Hard).

Leadership: House Captain and Valedictorian (Class 12); “The Red Coat” for all-round academic and co-curricular excellence; captain of the school Football and Volleyball teams.