

SURENDRA VISHWAKARMA

B.E. COMPUTER SCIENCE AND ENGINEERING

+91 7349628551 · surendrav.cs24@rvce.edu.in · www.linkedin.com/in/surendra-vishwakarma-95211a360 · github.com/surendra5153

EDUCATION

2024 – 2028

R V COLLEGE OF ENGINEERING

B.E. in Computer Science & Engineering
5th Semester
CGPA: 9.05

2022 – 2024

VISHWACHETANA VIDYANIKETA RESIDENTIAL PU COLLEGE

12th (PCMB)
Grade: 95.67%
JEE: 95.67 percentile
CET Rank: 840
COMEDK Rank: 1648

2022

SRI SHARANA BASAVESHWARA ENGLISH MED H S KARATAGI

10th
Grade: 99.2%

SKILLS

Languages: Python, C++, C, JavaScript, R
Frameworks: React.js, Node.js, Express.js, Flask, FastAPI, Celery
Web Tech: HTML, CSS, Tailwind CSS, Socket.IO, MERN Stack
Database: MongoDB, Postgres, ChromaDB, Redis
CS Fundamentals: Data Structures & Algorithms, OOP, Operating Systems, Computer Networks, System Design
Tools: Git, GitHub, Docker, Postman, VS Code, Ollama
AI & NLP: RAG, LLM Integration, PyTorch, scikit-learn, sentence-transformers, PyMuPDF, pdfplumber, Camelot
Concepts: REST APIs, JWT/OAuth Authentication, OCR, MCP, AI Agents, LSTM Anomaly Detection

LANGUAGES

English, Kannada, Hindi

ACHIEVEMENTS

- Solved 120+ Data Structures and Algorithms problems across coding platforms, building strong problem-solving fundamentals.
- Participated in the Meta PyTorch OpenEnv Hackathon.
- Published 6 public GitHub projects spanning full-stack, AI/ML and cybersecurity.

ABOUT ME

Computer Science undergraduate at R V College of Engineering (CGPA 9.05) who builds full-stack and AI-driven systems end to end, from React dashboards and Node/Flask/FastAPI backends to LLM-based RAG pipelines and LSTM anomaly detection. Solved 120+ DSA problems and strong in C/C++ implementations of core data structures. Seeking a software engineering internship to apply full-stack and applied-AI skills to real-world products.

PROJECTS

Annual Report Analysis System

- Built a fully local annual report analyzer (FastAPI, Celery/Redis, React/Vite) running LLMs via Ollama behind a provider-agnostic OpenAI-compatible client; turns PDFs into structured KPIs, risk flags and cited chat answers while keeping financial data on-device.
- Engineered two-pass extraction of 28+ financial KPIs (deterministic table scan with Ind AS aliases, LLM for narrative figures, then a verification pass) and a classifier for financial, regulatory, cyber, climate and supply-chain risks.
- Implemented hybrid RAG Q&A (ChromaDB semantic retrieval with keyword re-ranking, sentence-transformers embeddings) with conversational memory and page-level source citations.
- Built a Footnote & Consistency Engine, year-over-year anomaly detection and embedding-based peer discovery; cut PDF detection time from 10-15s to 3-5s (~3x) and LLM token usage by 60%.

GitHub: <https://github.com/surendra5153/annual-report-analyzer>

Shadow-OT – ICS/SCADA Deception Platform

- Built an ICS/SCADA deception and threat-intel platform of 15 Docker Compose services: Modbus TCP, SSH and SMB honeypots mirroring real PLCs, a Flask + Socket.IO API and a React dashboard for real-time monitoring.
- Implemented a PyTorch LSTM autoencoder (FastAPI microservice) that flags anomalous OT traffic by reconstruction error over 30-event sequences, with detections mapped to MITRE ATT&CK for ICS techniques.
- Developed an APT profiler (cosine similarity over 7 behavioral features against TRITON, Industroyer and Sandworm profiles), a SOAR playbook engine for automated isolation and alerting, and a STIX 2.1/TAXII 2.1 server for threat-intel sharing.
- Added a red-team Modbus attack simulator to test detection and auto-generated PDF incident reports.

GitHub: <https://github.com/surendra5153/shadowot>

Autonomous Coding Agent with Sandboxed Execution

- Building an autonomous coding agent with a write → run → observe → fix loop that executes LLM-generated code in an isolated Docker sandbox (no network, CPU/memory caps, hard timeout) under a capped retry budget.
- Adding test-driven execution, so generated code must pass a supplied pytest suite rather than just run, and an AST-based guardrail layer that blocks unsafe code (file-system access, network calls, process spawning) before it executes.
- Instrumenting every attempt (errors, retries, latency, token usage, guardrail blocks) to report task success and safety-block rates.

SkillSwap – Skill Exchange & Mentorship Platform

- Built a MERN skill-exchange and mentorship platform with Socket.IO real-time session chat, Jitsi video sessions via auto-generated password-protected meeting links, and Google/GitHub OAuth plus JWT authentication.
- Designed an explainable ML layer: linear-model skill recommender and mentor ranking with two-tier (process + MongoDB) caching and popularity fallback, TF-IDF cosine-similarity matchmaking, and logistic-regression session-success prediction.
- Added OTP-based college-email verification, gamification, learning roadmaps and an analytics dashboard; structured the Express backend into controllers, models and routes with a React (Vite) + Zustand frontend.

GitHub: <https://github.com/surendra5153/mainel>