Nookala Tejdeep

+91-9752520066 | tejdeep.dev | linkedin.com/in/tejdeepn | github.com/Tx-3011

Education

Manipal Institute of Technology Bangalore, India

B.Tech in Computer Science and Engineering ***(CGPA: 8.64)*** *2023 – 2027*

- **Relevant Coursework:** Data Structures & Algorithms, Database Management Systems, Operating Systems, Probability & Statistics, Computer Networks

Work Experience

Siemens Bangalore, India

Software Engineering Intern *2026 – Present*

- Building **agentic AI pipelines** to automate repetitive workflows across enterprise departments.
- Developing scalable backend automation by integrating LLMs, REST APIs, and internal enterprise systems.
- Collaborating with cross-functional teams to design, develop, and deploy AI-driven workflow automation solutions.

Technical Skills

Languages: Python (Pandas, NumPy, Scikit-Learn), Java, C, SQL (MySQL/PostgreSQL), JavaScript (ES6+)
Developer Tools: Git/GitHub, Docker, Linux, Flask, React, Node.js, MongoDB, Snowflake, Playwright
Core CS: Data Structures & Algorithms, Object-Oriented Programming (OOP), Enterprise Application Design, REST APIs
ML/AI: Random Forest, Generative AI (Gemini API), EDA, Feature Engineering, Data Analytics

Projects

PhishShield – AI-Powered Enterprise Security Tool | *Python, Flask, Google API, Gemini*

- Engineered a real-time phishing URL detection platform using **Flask** and **Gemini LLM APIs** for automated threat identification.
- Developed a scalable RESTful backend integrated with Google Safe Browsing to provide multi-layered security validation.

Playwright Test Automation Framework | *TypeScript, Playwright, GitHub Actions*

- Designed a production-ready E2E test framework using the **Page Object Model**, covering login, cart, and checkout flows.
- Implemented **storageState**-based authentication to bypass redundant login steps, reducing test runtime and flakiness.
- Configured a **GitHub Actions** CI pipeline to run cross-browser tests headlessly and auto-upload trace/HTML reports on failure.

Network Intrusion Detection System (NIDS) | *Python, Scikit-learn, Random Forest*

- Analyzed 125,000+ network traffic records to detect cyber threats using machine learning techniques.
- Performed feature engineering, preprocessing, and model optimization on high-dimensional network traffic data.
- Achieved a **96% F1-score** through hyperparameter tuning for accurate intrusion detection.

Certifications

Tools of the Trade: Linux and SQL – *Google*

Connect and Protect: Networks and Network Security – *Google*

Foundations of Cybersecurity – *Google*