K Harshit

kappalaharshith@gmail.com | **+91-9845198405**
github.com/karash10 | **linkedin.com/Kharshit** | **Harshit portfolio**

Summary

A detail-oriented Computer Science student passionate about the intersection of **Machine Learning**, **Deep Learning**, and **Cybersecurity**. I have hands-on experience developing advanced **DL models** and secure, scalable software solutions. Seeking a challenging role to apply these skills to solve complex problems.

Education

PES University, Karnataka, India
B.Tech in Computer Science and Engineering 2023 – 2027
CGPA: 8.7

Skills

Languages: Python, **Java**, C, JavaScript
Deep Learning & AI: PyTorch, **Hugging Face**, **Transformers**, **LangChain**, **LLMs**, **GANs**, **XAI**, NLP
Cybersecurity & Networking: Computer Networking, **Nmap**, **Socket Programming**, **JWT**, Ethical Hacking
Web Development & Database: React.js, **Node.js**, **MongoDB**, **FastAPI**, **Streamlit**, **Tailwind CSS**, **ChromaDB**
Tools & Core Concepts: Git, **Linux**, **Data Structures & Algorithms**, **APIs**

Work Experience

Summer Intern – CCNCS, PES University June 2025 – July 2025
Developed **XJailGuard**, an explainable framework for detecting advanced **multi-turn, cross-lingual jailbreak attacks** on **LLMs**. Authored a research paper on this work, selected for publication at the **ICICC Conference**.

Projects

XJailGuard : AI Safety Framework
Developed a secure multilingual AI assistant acting as a safety filtering layer for **LLM** deployment. Engineered to detect and block **prompt injection**, **multilingual attacks**, and **chained jailbreaks** in multi-turn conversations. Integrated an **XAI** module to provide token-level explanations for blocked content, ensuring transparency.
Tech Stack: Python, **PyTorch**, **Hugging Face**, **Transformers**, **XAI**, **FastAPI**, **Git**

CTI-RAG : CTI Analysis Chatbot
Designed a **Retrieval-Augmented Generation (RAG)** system for **Cyber Threat Intelligence (CTI)** analysis. Ingests and indexes CTI data (CVE, MITRE ATT&CK) into a vector database, enabling analysts to extract **actionable, cited intelligence** via a chatbot interface.
Tech Stack: Python, **LangChain**, **Gemini**, **ChromaDB**, **Streamlit**, **SentenceTransformer**

SecureLogger
A **cyber deception tool** to flood web server access logs with realistic, fake entries using a **GAN** (Generative Adversarial Network). The goal: **obfuscate true server activity** and frustrate attackers or unauthorized auditors.
Tech Stack: Python, **PyTorch**, **Flask**, Watchdog, Numpy, Logging

SecureSniff
A **network analysis tool** that **captures live packets**, generates detailed summaries including protocol breakdowns, source/destination information, and packet metadata. Integrated **Nmap** to perform **real-time scanning** on selected packets for vulnerability assessment. Combined packet inspection with **active network reconnaissance** to provide both passive and active security insights. Built with a focus on performance, usability, and security.
Tech Stack: Python, **Socket programming**, **NMAP**

PlayTogether : Full stack web application
Engineered a **full stack platform** for discovering, booking, and organizing sports activities and facilities. Implemented user authentication with **JWT**, venue booking, event management, and player connection features.
Tech Stack: React.js, **Node.js**, Express.js, **MongoDB**, **Tailwind CSS**, **JWT**

Certifications

Cybersecurity – Basics of red teamings
Learnt about the basics of **ethical hacking** in this course and got a certificate on completion of the course

Achievements and Extracellular

Awarded **Prof. C N R Rao Merit Scholarship** for ranking in the **top 25% SGPA holders** in the CSE department.