Harsh Jaiswal

Developer -1 Software Engineering

Mob: +91 7847952604 | Email: harsh.jaiswal@ust.com

Summary

- Backend development using Python and FastAPI, with scripting for automation and basic system monitoring.
- Full-stack development with REST APIs, React.js, TypeScript, and MongoDB/MySQL.
- Secure, scalable coding practices with Git-based version control.
- Hands-on experience with Generative AI, LLMs, and RAG applications.

Education

- Bachelor of Technology in Computer Science & Information Technology

Technical Expertise

- Python Full Stack
- React.js, TypeScript
- GenAI

Industry Experience

- Software Development

Professional Experience

- Experience building scalable backend systems using Python (FastAPI), with emphasis on clean, modular code, debugging, performance optimization, and secure coding practices.
- Strong full-stack development experience, integrating React.js and TypeScript frontends with Python backends, including RESTful APIs, authentication/authorization (JWT), and database interactions (MongoDB, MySQL).
- Proficient in using Git for version control, supporting collaborative development, branching strategies, and code reviews.
- Ability to automate environment setup, configuration, and basic system monitoring using Python scripts to support development and test environments.
- Experience supporting and administering application environments across Linux, Windows, and virtualized platforms, including VMware.
- Practical experience with deploying, testing, troubleshooting, and maintaining application services, as well as working with Generative AI and LLM-based solutions, including RAG pipeline implementation.

Project Details

Threat Intelligence Chatbot (RAG-Based AI System)

- Built an AI-driven threat intelligence chatbot using Retrieval-Augmented Generation (RAG) to respond to questions about malware, APT actors, and CVEs.
- Developed semantic search and document retrieval using ChromaDB vector database and ONNX-based embedding models to enable knowledge grounding.
- Integrated Azure OpenAI LLMs to produce contextually relevant and explainable responses based on the retrieved threat intelligence information
- Designed the outputs to be structured and aligned with the MITRE ATT&CK framework, including attack vectors, TTPs, impact analysis, and mitigation strategies.
- Enabled source attribution, data availability validation, and external enrichment with Tavily to provide concise and actionable intelligence to security analysts.