K Eswar Ashish

Andhra Pradesh, India
LinkedIn | GitHub
Email: ashish.171222@gmail.com | Mobile: +91-8106392251

I am deeply passionate about AI, Data Analysis, and full-stack web development, and I am committed to honing my skills in these areas. Concurrently, I am also actively exploring Deep Learning, DevOps, GenAI, Web3 and Cloud Computing to broaden my expertise. My dedication to ongoing learning and professional growth, along with a focus on emerging technologies in AI, drives my success in the tech industry.

Technical Skills

Languages	:	TypeScript, Python, Java, VHDL
Frameworks	:	React.js, Express, Node.js, Next.js, LangChain, Langgraph, TensorFlow, Scikit
Databases	:	MongoDB, PostgreSQL, Vector: ChromaDB, PineCone
Other skills	:	VLSI, Git, AWS, Azure

Education

Indian Institute of Information Technology Dharwad (IIITDWD) — Dharwad, Karnataka, India
Bachelor of Technology in Electronics and Communication Engineering, CPI: 8.69 — *2020 – 2024*

FIITJEE Junior College — Vijayawada, Andhra Pradesh, India
Intermediate Education, CGPA: 9.65 — *2018 – 2020*

Nirmala High School — Vijayawada, Andhra Pradesh, India
SSC, CGPA: 9.8 — *2008 – Dec 2018*

Work Experience

EDCULTS - AI Full Stack Research Intern — May 2024 to present

- Conducted data analysis on provided CSV files using libraries such as PandasAI and Chat2Plot to generate visualizations based on prompts.
- Developed and deployed serverless functions on Azure to create and manage APIs.
- Implemented a question generator from PDF documents, enhancing document comprehension and interaction.
- Applied various GenAi and prompt engineering techniques, including Retrieval-Augmented Generation (RAG), to improve AI model performance.
- Designed and implemented agentic framework for sales system for a sales bot using Langgraph
  * Two nodes acted as agents: one focused on providing sales information and the other on managing pricing and order processing.
  * Ensured seamless routing between the two agents by implementing a context buffer summary, which allowed both agents to share relevant session data and maintain a coherent interaction flow.
- Deployed serverless functions on Azure for Chat2Plot and salesbot functionality, significantly reducing operational costs, rather than traditional deployment.

Projects

GPS Spoofing Detection in UAVs — ***Machine Learning*** — Source Code

- A robust Python machine learning application was developed to classify signals into authentic and three types of spoofing categories. The application utilizes various machine learning algorithms including Decision Trees, Random Forests, Support Vector Machines (SVM), and Logistic Regression.
- Among these models, the Decision Tree algorithm demonstrated better classification of signals. The success of the Decision Tree model significantly contributes to the field of signal processing and security by enhancing the detection and mitigation of spoofing attacks.

Air quality surveillance and prediction

- This project employs an MQ2 sensor linked to a NodeMCU ESP8266 microcontroller, continuously sampling PM2.5 and CO gases and securely transmitting real-time air quality data to AWS IoT Core.
- Node-Red streamlines data integration with AWS, routing IoT data to S3 via IoT Core and Kinesis Streams. SageMaker deploys an LSTM algorithm, orchestrated with MLOps for automated data collection and training.
- Implemented a Node-Red UI for a live demonstration, providing real-time visualizations and updates of air quality changes

---

UAV Communication with RSA ***Cryptography, Web3*** Source Code

- An **RSA** based encryption for secure UAV communication with its ground station written in **JAVA**
- Communication encryption and decryption at sender and receiver side with dedicated **GUIs**

GRAB [In Progress] Source Code

- Building an innovative e-commerce platform supporting small transporters with AR integration (Blippar), blockchain development (Metamask, Ether.js, Motoko, Solidity), and secure features such as OAuth login and MongoDB storage for orders and products

Major Project

Countermeasure for FAA Remote ID spoofing GPA: 10, Project Report

- **Identification of Challenges:** The project starts by recognizing the challenges posed by the Remote ID requirement in UAV operations, particularly regarding privacy concerns.
- **Integration of SquidRID with ESP32 Boards:** SquidRID, a tool designed to test the FAA's Remote ID protocol, is integrated with ESP32 boards. This integration enables the creation of a simulated drone environment.
- **Data Collection and Analysis:** The integrated system allows for the collection of data related to UAV behavior, including identity and location information. This data is then analyzed to classify UAV activities effectively.
- **Machine Learning Algorithms:** Sophisticated machine learning algorithms are leveraged to differentiate between safe and potentially hazardous UAV activities based on the collected data. These algorithms are trained to recognize patterns and anomalies in UAV behavior.
- **Conclusion:** In conclusion, our project serves as a crucial security layer against Remote ID spoofing in UAV operations. Through the integration of SquidRID with ESP32 boards and the utilization of advanced machine learning algorithms, we not only address privacy concerns but also fortify UAV systems against potential threats. By differentiating between safe and hazardous UAV activities, our approach enhances security while ensuring the continued safe integration of UAVs across industries.