

AHSAN ALTAF

Researcher & Developer

@ahsanchattha145@gmail.com
ahsan-chattha-547086262

+923438413119
0009-0006-8356-9877

MR-AOH



EDUCATION

MS in Information Technology

Quaid-i-Azam University, Islamabad

2023 – 2025

Pakistan

CGPA: 4.0

BS in Information Technology

University of the Punjab, Lahore

2018 – 2022

Pakistan

CGPA: 3.25

WORK EXPERIENCE

Machine Learning / AI

2 years

Python Language

3–4 years

Visiting Lecturer

1 year TA

1.6 years

Quaid-i-Azam University, Islamabad

TECHNICAL SKILLS

- Programming Languages: Python, C++, JavaScript, SQL
- Machine Learning & AI: PyTorch, TensorFlow, Scikit-learn, Transformers, Hugging Face Transformers, LLaMA 3.2, Gemini, OpenAI, YOLO, OpenCV
- Blockchain & Security: Ethereum, Ganache, Solidity, Smart Contract, Nmap, Wireshark, Command-line security tools
- IoT & Embedded Systems: ESP32, ESP32-CAM, Arduino Uno, Sensors, Arduino IDE
- Development: HTML, CSS, React, React Native, Next.js, Streamlit, FastAPI, Django, Firebase, SQL, VS Code, Jupyter Notebook, Google Colab, Kaggle.
- Data Analysis & Visualization: NumPy, Pandas, Polars, Matplotlib, Seaborn
- Version Control: Git, GitHub

AREAS OF EXPERTISE

Machine Learning Artificial Intelligence Deep Learning Large Language Models (LLM)
Computer Vision Natural Language Processing (NLP) Data Science Privacy & Security

EXPERIENCE

A Hybrid Approach to IoV Security and Privacy: Combining SSI and LLM (MS Thesis)

Quaid-i-Azam University, Islamabad

📅 Jan 2024 – Feb 2025

📍 Pakistan

- Conducted research on blockchain technology and large language models (LLMs) for secure information sharing in smart vehicles.
 - Developed a prototype integrating Self-Sovereign Identity (SSI) and LLMs for enhanced vehicle security and communication.
 - Used Python, Ethereum (Ganache framework), cryptographic libraries, and LLaMA 3.2 3B for LLM integration.
-

Fine-tuning LLaMA 3.2 7B for Legal Text Summarization

Quaid-i-Azam University, Islamabad

📅 Nov 2023 – Jan 2024

📍 Pakistan

- Fine-tuned LLaMA 3.2 7B on a legal dataset for case summary generation and outcome prediction.
 - Utilized Hugging Face Transformers, PyTorch, TensorFlow, and DeepSpeed for model training and optimization.
-

Detecting Deception Based on Facial and Voice Features

Quaid-i-Azam University, Islamabad

📅 June 2023 – Oct 2023

📍 Pakistan

- Focused on lip and eyebrow movement analysis to optimize processing efficiency.
 - Used pre-trained model weights, OpenCV, NumPy, PyTorch, Scikit-learn, and TorchVision for facial and voice feature analysis.
-

Cybersecurity Vulnerability Scanner using LLMs

Quaid-i-Azam University, Islamabad

📅 Mar 2023 – May 2023

📍 Pakistan

- Developed a cybersecurity tool leveraging LLMs to scan target devices, identify vulnerabilities, and generate reports.
 - Integrated automatic inline commands, terminal-based applications, Nmap, XSS-script validation, and command-line tools.
 - Used Python and Gemini LLM for security analysis and vulnerability detection.
-

IoT-based Secure Smart Home Automation System

University of the Punjab, Lahore

📅 Dec 2021 – Oct 2022

📍 Pakistan

- Designed and implemented a smart home automation system with theft protection.
- Integrated face recognition, motion detection, and body detection.
- Utilized sensors including ESP32, ESP32-CAM, motion sensors, humidity/temperature sensors, gas sensors, and Arduino radar sensors.
- Used OpenCV, Mediapipe, YOLO for object detection and computer vision, Firebase for database management, Python, Arduino IDE and the Kivy framework for mobile app.

PUBLICATIONS

Empowering Smart Vehicles: Giving Authority with LLM and SSI

2024 International Conference on Frontiers of Information Technology (FIT)

📅 10.1109/FIT63703.2024.10838412

📍 Islamabad

- Focused on leveraging Self-Sovereign Identity (SSI) and Large Language Models (LLMs) for secure and autonomous smart vehicle systems.

Context-Aware IoV Security: A Decentralized User-Controlled Privacy-Preserving Multi-Layered Solution

📅 Submitted

📍 IEEE Internet of Things Journal

- Conducted research on blockchain and LLMs for secure information sharing in smart vehicles.
- Developed a prototype integrating Self-Sovereign Identity (SSI) and LLMs for enhanced vehicle security.
- Used Python, Ethereum (Ganache framework), Smart Contract, and LLaMA 3.2 3B.

Secure Smart Home: Federated Learning with LLM-Based Recommendations and Differential Privacy

Second Author

📅 Submitted

📍 EAI SmartSP 2025

- Designed a secure smart home system integrating federated learning and differential privacy.
- Developed LLM-based recommendations for enhanced user privacy and automation.
- Used Python, Fine Tuned llama 3.2 7B, and federated learning models.

Security Reference Architecture for Large Language Models

📅 Not Submitted yet

- Focused on mitigating the type of attacks that happen on LLMs. An architectural-based approach to adopt in order to overcome the attacks even on small models.

Detecting Deception Based on Facial and Voice Features

Second Author

📅 Not Submitted yet

📍 .

- Focused on lip and eyebrow movement analysis to optimize processing efficiency.
- Used pre-trained model weights, OpenCV, NumPy, PyTorch, Scikit-learn, and TorchVision for facial and voice feature analysis achieving 93% accuracy.

CERTIFICATIONS

- Introduction to Large Language Models - Coursera
- Generative AI with Large Language Models - Coursera
- Crash Course on Python by Google - Coursera
- Introduction to Cybersecurity Tools & Cyber Attacks - Coursera
- Foundations of Cybersecurity - Coursera
- Introduction to Computers and Operating Systems and Security - Coursera
- Programming with JavaScript - Coursera
- Introduction to Mobile Development - Coursera
- Developing Back-End Apps with Node.js and Express - Coursera
- Build a Full Stack App using React and Express - Coursera
- React Native - Coursera
- React Basics - Coursera