Manal Alsuwat

AI Engineer | Generative AI & LLMs | AI Agents | Applied AI Research

manal.s.alsuwat@gmail.com Saudi Arabia
linkedin.com/in/manal-alsuwat github.com/manal-alsuwat

PROFESSIONAL PROFILE

AI Engineer with a Master's degree in Artificial Intelligence and published research in self-supervised and multimodal learning. Hands-on experience building solutions powered by Large Language Models (LLMs) with Retrieval-Augmented Generation (RAG), LLM APIs, and multi-agent architectures, including context optimization layers that reduce inference cost while preserving accuracy. Skilled in evaluating and deploying AI systems with Python and modern AI frameworks, and in turning research concepts into practical applications.

CORE COMPETENCY AREAS

- Machine Learning Engineering.
- Generative AI, LLMs & AI Agents.
- Multimodal & Self-Supervised Learning.
- LLM Evaluation & Model Deployment.

PROFESSIONAL EXPERIENCE

King Khalid University
AI Excellence Fellowship — AI Researcher & Engineer | July 2026 – August 2026.
- Conducted applied research on LLM-driven automation for cybersecurity threat hunting.
- Designed and evaluated multi-agent LLM architectures on recorded attack datasets.

Taif University
Adjunct Lecturer | Computer Science Department | September 2024 – December 2024.
- Taught AI and computer science topics and guided students in implementing machine learning projects.

Imam Abdulrahman Bin Faisal University
AI Research Assistant | June 2021 – February 2023.
- Trained and evaluated deep learning models for deepfake detection.
- Prepared datasets and ran model experiments to support research objectives.

IEEE Access
Research Reviewer | September 2022 – October 2022.
- Peer-reviewed submitted manuscripts for technical accuracy, novelty, and scientific rigor.

Data Science Special Interest Group
Data Collector & Programmer | July 2020 – August 2020.
- Built preprocessing and clustering scripts for Arabic sign-language speech datasets.

EDUCATION

Umm Al-Qura University
Master's Degree in Computer Science — Artificial Intelligence | GPA: 3.97/4 with Honors | 2024.

Taif University
Bachelor's Degree in Computer Science | GPA: 3.72/4 with Honors | 2019.

SPECIALIZED TRAINING

- Agentic AI Bootcamp | Saudi Digital Academy (SDA) | May 2026.
- Professional Training in Generative AI | Generative AI Academy (SDAIA & NVIDIA) | May 2025.
- Samsung Innovation Campus — Artificial Intelligence Course | Samsung · Misk Skills | October 2024.
- Introduction and Advanced Artificial Intelligence Training | KAUST | November 2023 – January 2024.
- HCIA-AI V3.0 Course — Huawei Certified ICT Associate in Artificial Intelligence | Huawei | April 2023.
- Machine Learning Engineering Training | SDA | April 2020.

CERTIFICATIONS

- Microsoft Azure AI Fundamentals (AI-901) | July 2026.
- IBM AI Engineering Professional Certificate | December 2025.
- IBM Generative AI Engineering Professional Certificate | November 2025.
- NVIDIA Certified Associate: Generative AI Multimodal | July 2025.
- NVIDIA Certified Associate: Generative AI and LLMs | July 2025.
- AWS Certified Cloud Practitioner | January 2025.
- INE Jr Data Scientist Credential | November 2024.

PROJECTS

- **ContextShield AI — Context-Preprocessing Layer for Cheaper, Safer LLM Calls | 2026.**
  - Built a local, zero-LLM preprocessing layer: an adaptive router keeps only the context a request needs, redacts sensitive data, and isolates planted prompt-injection attacks, cutting input tokens by about 60% at equal accuracy.

- **ThreatHuntAI — Explainable Multi-Agent LLM Framework for Threat Hunting | 2026.**
  - Designed a five-agent LLM pipeline for analyzing Windows event logs and generating evidence-grounded incident reports.
- **Secure RAG Sales Agent — Retrieval-Augmented LLM Assistant | 2026.**
  - Built a RAG pipeline (LangChain, ChromaDB, Hugging Face embeddings) with an LLM-as-a-Judge security layer detecting prompt injection and jailbreak attempts.
- **Master's Thesis — Multimodal Data Representation using Self-Supervised Learning | 2024.**
  - Implemented self-supervised learning techniques to generate robust audio-visual representations, improving accuracy in sound classification tasks.

PUBLICATIONS

- Spatial-Temporal Self-Supervised Learning for Audio Classification — 2025.
- Audio–Visual Self-Supervised Representation Learning: A Survey — 2025.
- Comparative Analysis of Machine Learning Algorithms for Predicting Drug Mechanism of Action — 2025.
- A Deepfake Face Mask Dataset for Infectious Disease Era with Deepfake Detection Algorithms — 2023.
- Prediction of Diabetic Retinopathy Using Convolutional Neural Networks — 2022.
- Makkah Landmark Recognition Using Deep Learning — 2022.
- Detection of Cardiovascular Disease Using Machine Learning Classification Models — 2021.
- A Survey of the Application of Artificial Intelligence on COVID-19 Diagnosis and Prediction — 2021.
- A Hybrid Model Based on Radial Basis Function Neural Network for Intrusion Detection — 2020.

AWARDS

- 1st Place — Speech Clustering for Arabic Sign Language | Data Science Special Interest Group | 2020.
- 1st Place — Best Arabic Research Content | Etalem Tech Group | 2018.

SKILLS

AI & Machine Learning: Deep Learning, AI Agents, Transformers, LLMs & RAG, Self-Supervised Learning.
Data Science & Analytics: Data Preprocessing, Feature Engineering, Model Evaluation, Data Visualization.
Programming & Tools: Python, PyTorch, TensorFlow, Keras, OpenCV, LangChain, ChromaDB, Git.
AI Systems & Deployment: LLM Evaluation, LLM APIs, Prompt Engineering, Hugging Face, AWS, Azure.
Languages: Arabic (Native), English (Fluent).