

Mohamed Ajab

MSc Advanced Computer Science | AI and agent security

Leicester, UK | 07470 168482 | Mohamedajab8@gmail.com
github.com/Mohamedajab | UK Home-fee eligible

PROFILE

First-Class Computer Science graduate completing an MSc at Loughborough University. My dissertation focuses on controlled multi-turn evaluation of LLM behaviour. I am seeking PhD research in AI and agent security, particularly prompt injection, agent hijacking and runtime safeguards.

EDUCATION

Loughborough University | MSc Advanced Computer Science | 2025-2026

Excellence Scholarship. Research Methods: 85%; Robotics and Intelligent Systems: 70%.

De Montfort University | BSc (Hons) Computer Science | First Class, 2025

Big Data and Machine Learning: 83%; Development Project: 71%; Privacy and Data Protection: 69%.

RESEARCH AND TECHNICAL PROJECTS

Multi-Turn LLM Safety Evaluation Benchmark | MSc dissertation, 2026

- Designed a controlled six-turn benchmark comparing fixed LLM endpoints across scenarios, context conditions and repeated runs, separating pilot evidence from dissertation data.
- Implemented model calling, annotation and TF-IDF/SVD analysis, with append-only evidence, offline validation and automated tests. Python, OpenRouter, Streamlit and Pydantic.

AgentGuard | Prompt-Injection Security Benchmark, 2026

- Developed an AI-assisted, single-step sandbox comparing baseline, content wrapping, detector quarantine, tool policy and combined controls, using only fictional local tool actions.
- Added a frozen 22-case synthetic challenge, five-arm ablation and repeated runs on two hosted models, reporting API failures, uncertainty and legitimate-tool utility.

github.com/Mohamedajab/agentguard-lab

PhishGuard | Machine-Learning Phishing Detector, 2026

- Compared word and character TF-IDF with logistic regression, using body-template grouped cross-validation and training-only threshold selection.
- Added ROC/PR curves, error review and external-schema loading. Documented synthetic-data leakage and the gap between perfect training CV and weaker challenge results.

github.com/Mohamedajab/phishguard-ml

AI Volleyball Performance Analyser | BSc dissertation, 2025

- Developed player detection/tracking and jersey-number recognition using YOLO, OpenCV and EasyOCR, with a Streamlit interface for reviewing processed match footage.

github.com/Mohamedajab/volleyball_detector

SELECTED SIDE PROJECTS

SplitCheck (dataset leakage checks); RunLedger (hash-linked experiment records); Service SLO Lab (availability and latency budgets); Tool Policy Playground (default-deny action rules).

TECHNICAL SKILLS AND RELEVANT STUDY

Python, pandas, NumPy, scikit-learn; OpenRouter, Streamlit, Pydantic, httpx; TF-IDF, SVD, logistic regression and Plotly; YOLO, OpenCV, EasyOCR; pytest, Ruff and Git.

Relevant study: Artificial Intelligence, Applied Cryptography, Network and System Security, Agent-Based Systems and Computer Vision.

MSc dissertation repository is private; code available on request.