Muhammad Moosa Bin Naseem

Software Engineer · Data Scientist

+92 331 2140037 | moosa.binnaseem09@gmail.com | unholymoses.site | unh0lymos3s | moosabinnaseem

Skills

Deep Learning Frameworks	Pytorch, TensorFlow
Generative AI and LLMs	HuggingFace Transformers, Ollama, Litellm, Open router, Agents, MCP
Programming Languages	Python, C++, Rust, Go, Ts
MLOps and Quantization	Docker, Llama.cpp, ONNX, MLFlow
Back-end and Networking	Flask, Tokio, Node.js, TCP/UDP, REST
Systems and Security	Linux Systems Administration and hardening, Dynamic/Static Application Testing

Work Experience

Virtual Remittance Gateway (VRG) — AI Research and Development, GRC

Karachi, Pakistan

Data Scientist — *December 2024 — Present*

- Built a full stack analytics engine serving different dashboards of **State Bank of Pakistan's Asaan Mobile Account & Agent-Interoperability Scheme**, REST APIs and an LLM Chat Assistant ; with React, Node.JS/Express, Python and Oracle.
  - Utilized **Python+Oracle** data pipeline to join transaction tables of >30M and >14M rows into an aggregated json snapshot reducing load time from **≈60 seconds to < 1 second .**
  - Built an Agentic Chat Assistant using LLM tool calling with **Ollama**; wrote 6 different tools for data-retrieval, with a multi-tool call loop, thread-based session persistance, and **SQLite DB** for chat history storage and restarts.
  - Implemented layered guard-rails for AI security against hallucination and prompt injection: a Pre-flight LLM classifier to detect the scope of queries, and hardened system prompt boundaries to ensure tool-returned answers.
  - Built a client side geospatial Agent-Locator utility using **Deck.gl, MapLibreGL and SuperCluster** to track activity of AIO Agents across Pakistan.
- Worked on training the core ML model VRG's Fraud Detection system
  - Prepared and labelled Millions of transactions for Machine Learning
  - Parallelized the training phase by using bayesian optimization techniques with **Optuna Studies**.
  - Implemented a Model Registry with ML flow for dynamic model selection, thresholding, evaluation and fallbacks in case of degraded performance.
  - Achieved over **87%** accurate predictions, Performed in depth evaluation of each iteration to discover caveats in the dataset and shortcomings of the ML model.
- Aggregated cash-in and cash-out events from all MBE ATM Terminals in Canada into a single dataset, and wrote a created an LSTM based Deep-Learning model to accurately and preemptively forecast stale-cash losses and cash-out events.
- Built an internal suite utilizing **Python/Flask framework** to automate daily reporting for State Bank of Pakistan and partner banks for regulatory compliance.
- Working closely with Cybersecurity team to perform vulnerability assessment of in-house apps with **SAST & DAST** tools
- Relying on AI coding tools **ClaudeCode, OpenCode, Codex** for rapid prototyping, exploring new technologies and creating secure-by-design applications.

Askari Technologies — Software Engineering Team

Karachi, Pakistan

Junior AI Developer — *August 2024 — September 2024*

- Developed multiple end-to-end AI, Quant and software solutions for different international clients
- Built and Deployed a RAG pipeline for **Telecof**, for FAQs and appointment booking via WhatsApp using **Twillio** for WhatsApp services and **LangChain** for Agent development with a **ChromaDB** KnowledgeBase.
- Wrote a middleware to connect SierraCharts with MetaTrader5
  - Wrote SierraCharts Custom studies using **ASCIL & C++** to read and aggregate chart Data from sessions.
  - Wrote a C++ API to serve aggregated data over a web server.
  - Developed an Expert Advisor for MetaTrader5 with Python and MQL5 to visualize patterns in an MT5 terminal
- Fine-tuned GPT-2 to generate Arabic poetry for an educational institution, deployed using **IBM Watson**
- Built a bot to scrape and share trending videos from Youtube and Facebook using **Youtube Data API and GraphAPI**

Gerry's — Software Engineering Team

Karachi, Pakistan

Web Development Intern — *Fall 2023*

- Wireframed and Developed the frontend for Gerry's official website
- Worked on developing the frontend for a Gerry's group subsidiary

JS Bank Ltd. — Ancillary Apps Development

Karachi, Pakistan

Data Engineering Intern — *Summer 2016*

- Wrote **SQL Queries** for Ad Hoc data extraction and manipulation
- Worked on **Microsoft SSIS and SSMS** to perform ETL processes and aggregations

Projects

Hades: AI Based intrusion detection system *(Paper)*

Undergraduate Researcher

- Worked on core model training using LSTM-AE for feature compression and Catboost algorithm for classification
- Fine tuned and compared the hybrid learning technique with different machine learning algorithms
- Wrote backend services to transmit flagged IPs over to the dashboard

Dorq: AI Powered Backtesting Engine *(Link)*

Software Engineer

- Built Dorq, an AI powered backtesting engine, that generates strategies from macroeconomic research papers.
- Utilizing SmolDocling to parse and extract information from documents.
- Ollama powered locally hosted, custom AI Agents to generate a strategy spec and code. Along with a Chat Agent to provide support about the strategy.
- Backtesting engine powered by custom agents and Alpaca Paper trading API as tooling.
- using yFinance API to fetch live data according to spec.
- Built a user friendly interface, with Actual vs Prediction Graphs to visualize backtesting results.
- **Technologies: Python, IBM SmolDocling, Ollama, React.js, Alpaca , yFinance**

Pinkeye: Cyber kill-chain harness for security professionals *(Link)*

Software/Security Engineer

- Building Pinkeye, an open source agentic harness for automating Network Recon/VAPT/Exploitation
- Writing custom tools for **NMAP, ZAP, FFuF, Nikto, Nuclei**.
- Integrating threat and Ioc detection APIs, from **VirusTotal, MIPS, GitLeaks.**
- Wrote a MetaSploit RPC Client to ensure attack capabilities.
- Implementing different **Agent-Personalities** e.g (Recon, Attack, etc.). Also implementing **Inter-Agent communication** to make the agents work in a team rather than independently.
- Writing strong system prompts. to ensure authenticity and implemnting control-flow patterns to validate LLM responses to minimize hallucinations.
- Implementing a strict scope-guard, that ensures the Agents remain attacking the allowed hosts for an engagement.
- Implementing a disposable, containerized architecture to keep the agents sandboxed.
- **Technologies: TypeScript, React, Python, Open-Source Cybersec tools**

Forex Trend Prediction Model

Data Scientist

- Built a Forex prices and trend predictor using Bi-Directional LSTMs, achieving high accuracy over short term predictions
- Built the Neural Network using **PyTorch**, collected data on demand using **yFinance** and an interactive frontend with **Tkinter**

DOOM AI Agent

Data Scientist

- Trained an Agent via Reinforcement Learning to play the iconic DOOM 1993
- Utilized **Stable Baselines 3** to train the agent using **PPO** algorithm
- Used **VizDOOM** for environment models and **TensorBoard** for Visualization

Education

BS in Computer Science *Karachi, Pakistan*

Institute of Business Management, Karachi *2020 — 2024*

- **Relevant Coursework—** Machine Learning, Data Science and Analytics, Software Engineering, Computer Security, Programming Language Theory, Compiler Theory, Operating Systems and Networking, Cryptography, Networked and Distributed Systems
- **Thesis—** AI based Intrusion Detection System using Hybrid Learning