

Dawit Abdisa

Software Engineer | AI Engineer | Cybersecurity |
Solution Engineer



Research Fit

Software engineering MSc candidate at USTC with hands-on work across LLM applications, retrieval-augmented generation, agentic workflows, prompt-injection testing, and applied cybersecurity. I build practical AI systems end to end, then probe their failure modes, safety controls, and evaluation gaps. My PhD goal is to study how autonomous LLM-based agents can be made more robust against prompt injection, jailbreaks, unsafe tool use, and adversarial manipulation while remaining useful in real-world deployments.

Research Interests

- Primary** Agentic AI security, LLM security, prompt injection defense, adversarial evaluation of autonomous agents, safe tool-use orchestration, and secure RAG systems
- Methods** Agent benchmarking, red teaming, guardrail design, retrieval and tool-use policy controls, full-stack experimentation, security testing, and evaluation-driven iteration

Education

- 2023 – Jan 2027 **MSc in Software Engineering, University of Science and Technology of China (USTC)**
Coursework and project work spanning AI systems, software engineering, data systems, security practice, and applied digital product development.
- 2019 – 2023 **BSc in Computer Science, Changzhou University**, GPA: 4.7/5.0; ranked 1st in major and class
China Scholarship Council (CSC) Award; strong record in software engineering, leadership, and cross-cultural academic engagement.
- 2021 **Selected Academic Programs, Tsinghua University / Qingdao University**
Global Summer School: Innovation for SDG; Innovation & Entrepreneurship in the Digital Economy; Chinese Language Studies.

Research Project

- 2026 **Master's Thesis Project, University of Science and Technology of China (USTC)**
Developed an AI-driven decision-support system for PV and battery energy storage feasibility analysis, integrating multi-agent workflow orchestration, geospatial and solar resource assessment, scenario-based sizing, financial modeling, and automated reporting.

Technical Experience

- 2025 – Present **Energy Solution Engineer, Wanbang Digital Energy (StarCharge)**, International Solutions Center
- Work across complex software-enabled energy systems, translating operational requirements into implementable technical solutions and coordinating with engineering teams.
 - Strengthened systems thinking, reliability reasoning, and stakeholder communication while working on safety-critical power and infrastructure scenarios.
 - Contributed technical analysis, presentations, and solution refinement across customer-facing projects involving distributed energy, storage, and charging systems.
- 2017 – 2023 **Full-Stack Software Engineer & Client Lead, EthioWeb Digital Solutions**, Remote / Client-facing delivery
- Led end-to-end development of 15+ web products, covering requirements discovery, system design, implementation, debugging, deployment, and client delivery.
 - Built experience shipping usable systems under real constraints, which now informs how I prototype and evaluate AI-enabled applications.
 - Worked across frontend, backend, databases, APIs, and production support, giving me a practical foundation for agent-enabled software experimentation.

- 2020 – 2023
- Teaching Assistant, Changzhou University International Student Office**
 - Supported multilingual communication, translation, and coordination among international students, faculty, and staff.
 - Built concise technical communication habits useful for research collaboration, presentation, and cross-cultural academic work.

Selected AI Security & Agentic Systems Projects

- 2025 – 2026
- Prompt Injection Scanner**
 - Built a CLI tool to test LLM system prompts against 22 categorized prompt-injection payloads with both keyword and LLM-judge evaluation modes.
 - Evaluates jailbreak, role-play bypass, and data-extraction attack patterns to identify weak prompt boundaries and unsafe model behavior.
 - Repository: github.com/helloworldceo/prompt-injection-scanner
- 2025 – 2026
- Todo & Email Automation Agent**
 - Built an agentic assistant with LangGraph, Gmail API, and Streamlit that manages to-do workflows while reading, drafting, and sending emails across multi-step reasoning loops.
 - Practical experience with agent state, tool invocation, workflow orchestration, and the security implications of autonomous action-taking.
 - Repository: github.com/helloworldceo/todo-email-automation-agent
- 2024 – 2026
- Conversational RAG Assistant**
 - Built a retrieval-augmented assistant with LangChain LCEL, ChromaDB, Streamlit, LangSmith tracing, and RAGAS evaluation support.
 - Explored grounded question answering, retrieval quality, traceability, and evaluation loops relevant to secure and trustworthy LLM deployments.
 - Repository: github.com/helloworldceo/rag-assistant
- 2023 – 2025
- Applied Security Tooling**
 - Built an intentionally vulnerable Flask web app with documented SQLi, XSS, and IDOR issues plus exploitation notes and secure remediation guidance.
 - Built a network traffic analyzer using Scapy to detect scanning behavior and cleartext credential leaks from live interfaces or PCAP files.
 - Completed hands-on web security testing in Docker-based SEED lab environments covering CSRF, XSS, SQL injection, SSL/TLS, and related attack surfaces.
- 2023 – 2025
- AI / ML Foundations**
 - Built an EEG-based driver drowsiness classification pipeline comparing SVM, LSTM, and KNN, with SVM reaching 98% accuracy.
 - Studied transformer architectures and generative modeling through NanoGPT training and analysis work involving GPT-, BERT-, and ELMo-related concepts.

Technical Skills

LLMs & Agents	LLM applications, RAG pipelines, LangChain, LangGraph, agent workflows, prompt engineering, evaluation loops, tool orchestration
Security	Prompt injection testing, web security, penetration testing labs, secure design thinking, network traffic analysis, adversarial mindset
Software	Python, JavaScript, SQL, HTML, CSS, React, Node.js, Streamlit, API integration, Git, Linux, Docker
Data & Evaluation	ChromaDB, LangSmith, RAGAS, data analysis, visualization, experiment iteration
Languages	English (Fluent), Chinese (HSK 4), French (B1), Amharic (Native), Afaan Oromo (Native)

Honors & Additional Information

- Awards
- CSC Award; 3rd Prize, World Vocational College Skills Competition (Maze Robot); Outstanding Student Leader
- Recognition
- Featured in CGTN, CCTV1, and China Daily; 25+ academic honors and certifications highlighted in portfolio materials.
- Location
- Currently based in China.

Contact

Phone: +86 132 3517 8205
Email: davidabdisa40@gmail.com
WeChat: Helloworld_Ceo

Portfolio: helloworldceo.github.io
LinkedIn: linkedin.com/in/dawit-abdisa-44915518a
GitHub: github.com/Helloworldceo