ALBERT YOSHIMOTO

El Paso, TX | (915) 731-4379 | ayoshimoto@miners.utep.edu
linkedin.com/in/albert-yoshimoto | github.com/atyoshi | atyoshi.github.io

EDUCATION

University of Texas at El Paso | M.S. in Artificial Intelligence | GPA 4.0 | Expected May 2027

Coursework: Machine Learning, Decision Making in AI, Advanced Algorithms, Computer Security, Software Architecture

New Mexico State University | B.M. Instrumental Performance | GPA 3.85 | May 2023

RESEARCH EXPERIENCE

Army HBCU-MI SPARK | Research Fellow | Summer 2026

• Conducted CyberAI research; co-developed capture-the-flag scenarios and infrastructure with ARL and TDAC.

• Contributed to ModelScope, a modular evaluation platform for autonomous agents using ground-truth assessment criteria.

Cybersecurity Rapid Innovation Group (CyberRIG), UTEP | Research Assistant | 2026–Present

• Prototype AI-driven cybersecurity tools and contribute to practical security exercises and research workshops.

SELECTED TECHNICAL PROJECTS

Blue Cheese | Python, Suricata, Linux, Docker

• Implemented Suricata JSON alert ingestion and normalization into structured records for downstream analysis.

• Designed a modular multi-agent workflow for triage, correlation, investigation and reporting; live ingestion in development.

SpecGuard | Python, RAG, ChromaDB

• Built a vulnerability-analysis framework combining static analysis, LLM reasoning and retrieval over 1,999 CVEs.

• Implemented detection logic for memory corruption, use-after-free and integer overflow; built ground-truth evaluation.

LLM Uncertainty Signals for Cybersecurity Analysis | Python, Machine Learning

• Investigating confidence and token-level uncertainty as predictors of LLM correctness in cybersecurity scenarios.

• Designed evaluation with logistic regression, shallow trees, AUROC, Brier score, calibration and feature ablation.

ModelScope | Autonomous-Agent Evaluation

• Designed plugin-based agent evaluation and metrics for task success, runtime, resource usage and policy compliance.

TECHNICAL SKILLS

Languages: Python, Java, SQL, JavaScript, PHP

AI/ML: scikit-learn, regression, decision trees, model evaluation, RAG, LangChain, ChromaDB, Ollama, llama.cpp

Security/Systems: Suricata, network analysis, vulnerability assessment, Linux, Docker, Git, Wireshark

CERTIFICATION

Google Cybersecurity Certificate (Coursera, 2025)