LOUIS IACOLETTI
Applied AI Engineer | AGI-Augmented Systems & Adversarial NLP
Fairfax, VA
GitHub: louis57xl-coder

PROFESSIONAL SUMMARY

Applied AI Engineer building secure, deterministic, and production-ready AI systems by strategically augmenting software engineering expertise with frontier AGI platforms. Specializes in hardening, safety-testing, and deploying full-stack AI applications with emphasis on reproducibility, adversarial robustness, and ethical deployment.

If you have a good idea for a useful AI application compiled to run on a Windows 11 computer, or just need someone talented enough to help you develop the software needed to make it happen, I would like to hear from you? This type of work is orders of magnitude easier when you leverage the power of AI to your advantage!

SELECT ACHIEVEMENTS

• Built and deployed a fraud-detection AI application achieving **94.2% accuracy** and packaged as a user-facing standalone executable.
• **Scored in the 96th percentile** on the Gemini Advanced Reasoning Benchmark for Applied AI Engineering (outperforming 96% of engineering candidates).

CORE COMPETENCIES

AGI-Augmented Engineering

• Human-in-the-loop orchestration for accelerated design & reasoning using controlled LLM calls.
• LLM-assisted code generation, adversarial prompt testing, and multi-step reasoning chains with validation layers to eliminate hallucinations.
• Prompt/output versioning (git-tracked YAML/JSON) for full reproducibility and

auditability.
• Cross-model API orchestration (OpenAI GPT, Gemini/Advanced, Grok, DeepSeek) with fallback/ensemble logic.
• Deterministic model configuration: fixed seeds, pinned weights, environment isolation, and granular logging (MLflow/structlog).

Machine Learning & Deep Learning
• PyTorch: Custom nn.Module design, training hooks, optimizer tuning, mixed-precision training (AMP).
• Hugging Face Transformers: Fine-tuning, embeddings, token-level analysis, and semantic similarity.
• Advanced training: Weighted loss, focal loss for imbalance, probabilistic calibration, uncertainty estimation.

Safety & Adversarial NLP
• Refusal-pattern mining, guardrail bypass probing, and red-team evaluation using adversarial datasets.
• Behavioral signal extraction: manipulation, coercion, urgency tactics, and social-engineering detection.
• Longitudinal harm modeling via time-series embeddings and sequence classification.

Tools & Platforms
Python · PyTorch · Hugging Face · OpenAI API · Gemini API · Grok API · DeepSeek API · Git · Docker · MLflow · WandB · PyInstaller · uv/Poetry

Evaluation
• **96th percentile** on Gemini Advanced Reasoning Benchmark for Applied AI Engineering.

AI SAFETY PROJECTS & PROTOTYPES
(Detailed code, commits, and releases: louis57xl-coder)

ScamCheck v2.01 – Open Source Python Project | AI-Scam-Detection
[Primary Project · 80+ commits · v2.01]
Goal: Real-time detection of relationship scams, romance fraud, pig-butchering, and law-enforcement impersonation in text.
Solution: End-to-end Python/PyTorch CLI tool (scamcheck.py) using a hybrid detection engine:
• **Heuristic matching:** 200+ keyword patterns across sliding windows for love-bombing,

urgency, money requests, and grooming.
• **ML analysis:** Hugging Face emotion pipeline (j-hartmann/emotion-english-distilroberta-base) for fear/joy/sadness signals.
• **Production-grade deployment:** Packaged as standalone executable via PyInstaller; includes REST API endpoints, **Docker-optimized container (v2.01)**, GPU acceleration, and non-root user execution for enhanced security.
• **Deterministic execution:** Environment isolation, dependency pinning, and reproducible builds.
Results: Achieved **94.2% accuracy**, **92.5% precision**, **91.8% recall**, **92.1 F1** on mixed datasets.

HarmTrace | Longitudinal Abuse Detection Model
Built with PyTorch sequence models to track cumulative abuse signals (grooming, financial exploitation, escalation) over time. Uses time-series embeddings and weighted-loss optimization for high-recall detection in streaming contexts.

IntentGuard | Manipulation-Detection Engine
Identifies psychological-pressure markers (engineered guilt, false scarcity, gaslighting) via AGI-augmented orchestration. Leverages custom PyTorch modules and cross-LLM behavioral extraction for real-time risk scoring.

ConsentLens | Consequence-Aware NLP System
Exposes downstream legal, financial, and emotional consequences prior to user consent. Uses Transformers for consequence extraction, probabilistic framing, and integrated safety guardrails to prevent manipulative outputs.

All systems emphasize ethical AI principles: hallucination mitigation, prompt/output audit trails, red-team hardening, deterministic execution, and explainable outputs.

ENGINEERING PROFILE
Applied AI Engineer pursuing graduate Computer Science specialization in Machine Learning/Deep Learning at George Mason University. Combines a background in large-scale systems architecture, security oversight, and high-reliability delivery with a dedicated focus on building hardened, AGI-augmented AI applications. Tenacious and detail-oriented; expert in full environment isolation, strict dependency pinning, deterministic builds, and granular change tracking.

PRIOR SYSTEMS EXPERIENCE

Senior Systems Architect / Engineering Lead

• Directed multidisciplinary teams delivering mission-critical, high-reliability platforms.
• Led architecture, deployment, modernization, security oversight, and configuration control for large-scale systems.
• Deep experience in systems hardening and reproducibility directly informs current ML/AI pipeline design for safe, production-grade deployment.

EDUCATION

• **Graduate Computer Science – AI / Deep Learning Focus** (Active) – George Mason University
• **M.S., Information Systems & Software Engineering** – George Mason University

---