LOUIS IACOLETTI
Applied AI Engineer | AGI-Augmented Systems & Adversarial NLP
Fairfax, VA
Email: Louis57xl@gmail.com | Phone: 202-790-2347
GitHub: [louis57xl-coder (Louis Iacoletti)]

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.

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 **91st percentile** on the Gemini advanced reasoning benchmark for applied AI engineering.

CORE COMPETENCIES

AGI-Augmented Engineering

• Human-in-the-loop orchestration for accelerated design & reasoning using controlled LLM calls (temperature=0 deterministic mode).
• 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-4o/o1, Gemini 1.5/Advanced, Grok, DeepSeek-V2) 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 (AdamW, Lion), 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/Nuitka · uv/Poetry`

Evaluation
• 91st percentile on Gemini advanced reasoning benchmark.

AI SAFETY PROJECTS & PROTOTYPES

(Detailed code, commits, and releases: [louis57xl-coder (Louis Iacoletti)]

ScamCheck | AI-Powered Fraud Detection CLI `[Primary Project · 71+ commits · v1.12]`
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:** 100+ 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.
- Weighted scoring system (Low–Critical), explainable AI breakdowns, color-coded terminal interface, and interactive CLI loop.
  Deployment: Packaged as standalone `scamcheck.exe` via PyInstaller; includes REST API endpoints, Docker support, and GPU acceleration.
  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