

SAKSHAM KAPOOR

Email: sakshamk@umd.edu | **LinkedIn:** [linkedin.com/in/saksham-kapoor-umd](https://www.linkedin.com/in/saksham-kapoor-umd) | **GitHub:** github.com/SakshamKapoor2911

PAGE 1: EXECUTIVE PROFILE & CORE EXPERIENCE

Computer Science & Machine Learning Engineer · AI + X across Multiple Verticals

Architect of intelligent, scalable systems at the intersection of AI and high-impact domains. Specializing in mechanistic interpretability, real-time streaming architectures, autonomous multi-agent systems, and high-throughput microservices — with applied research across Healthcare, Security, FinTech, HCI, and more.

🎓 EDUCATION & FELLOWSHIPS

- **University of Maryland, College Park** | *Expected December 2027 B.S. in Computer Science & Machine Learning (Social Data Science Track)*
 - **Honors/Fellowships:** AI/ML Fellow (Break Through Tech AI at Cornell), Handshake MOVE Scholar, AWS Scholar
 - **Academic Leadership:** VP Big Th!nk AI (1,500+ member organization), VP SALC

🔧 TECHNICAL SKILLS MATRIX

- **Languages & Frameworks:** Python, Go, C#, Java, TypeScript, PyTorch, PyTorch Lightning, .NET 8, Spring Boot, React, React Native, Node.js, Deno, LangGraph, WebGL
- **Systems & Infrastructure:** Kubernetes (GKE), Docker, AWS (SQS, DynamoDB, Bedrock, S3, SageMaker), Redis, PostgreSQL, Raft Consensus, ClickHouse, NATS JetStream, Polygon L2, Arweave
- **AI & Interpretability:** TransformerLens, WhisperX, SAM 2, Transformers (RoBERTa, BERT), OpenCV, GANs, LLM Fine-tuning (GRPO, LoRA), Pyro, DoWhy, XGBoost, FinBert
- **GIS & Visualization:** GeoPandas, GDAL, Rasterio, Mesa (Agent-Based), D3.js, React Three Fiber (R3F), Three.js, Mapbox GL JS, LaTeX

📁 PROFESSIONAL EXPERIENCE

Trufflow | *Machine Learning Engineer Fellow* | **Sep 2025 – Dec 2025**

- **Real-Time Monitoring:** Built an enterprise anomaly detection system handling 1M+ events/sec peak load utilizing Polars data pipelines.
- **Precision Optimization:** Designed a graph-aware model mapping component topology, achieving a 73x PR-AUC improvement over static baselines.
- **Debugging Workflows:** Replaced static thresholds with relative deviation scaling, resulting in a 28x debugging speedup.

- **Video Segmentation:** Optimized a SAM 2 pipeline automating behavioral coding, reducing video processing time from 105 to 19 minutes.
- **FFmpeg Speech Pipeline:** Coordinated end-to-end speaker diarization integrating WhisperX and pyannote.audio for 100+ dyadic sessions.
- **Sentiment Contagion:** Fine-tuned RoBERTa models to analyze emotional synchronization using Linear Mixed Effects Models in R.

Saksham Kapoor — Page 1/7

PAGE 2: AI ALIGNMENT, SAFETY & INTERPRETABILITY

Vertical Focus: Circuit Stability · Mechanistic Interpretability · Autonomous Alignment Agents

Dedicated to dissecting the internal representations of deep learning models, auditing agent execution pathways, and building self-healing alignment mechanisms to prevent cognitive failure modes in production. Current research includes circuit-level stability analysis and sycophancy failure modes in reasoning LLMs.

SPECIALLY FEATURED TOOLKIT

- *TransformerLens, PyTorch, LangGraph, Gemini 2.5 Flash, Playwright, axe-core, CUAD datasets, Residual Stream Patching*

COMPONENT PROJECTS

1. **calculated-liar-mats · Mechanistic Interpretability Alignment Research**

- **The Discovery:** Identified a novel "Calculated Liar" failure mode where Qwen-2.5-1.5B-Instruct correctly computes math steps in its Chain-of-Thought (CoT) but flips the final answer to satisfy a high-authority sycophantic persona.
- **Key Achievements:**
 - Avoided metric mirage from coarse layer-10 patching by pivoting to position-specific residual stream ablation.
 - Executed surgical ablations on persona tokens (positions 0–4) using **TransformerLens** to restore behavioral honesty without accuracy collapse.
 - Isolated a dedicated attention head circuit in layers 9 and 10 responsible for propagating persona constraints to deduction nodes.

2. **SecondSight · Autonomous Accessibility Repair Agent**

- **The Innovation:** An "Action Era" agent that autonomously audits live websites, traces WCAG violations to source components, writes self-healing patches, and opens pull requests — replacing a manual review process.
- **Key Achievements:**

- Built a live audit pipeline running axe-core and Playwright inside a dynamic LangGraph multi-step workflow.
- Implemented DOM-to-source code mapping with **Gemini 2.5** to pinpoint visual WCAG errors to specific Next.js files and line numbers.
- Designed a 3-attempt compile-verify loop that automatically pushes branch commits and creates final GitHub PRs.

3. CounterPoint AI · Adversarial Multi-Agent Debate Simulation

- **The Innovation:** A stress-testing platform utilizing LangGraph to simulate adversarial debate paths and evaluate prompt robustness and safety parameter drift.
- **Key Achievements:**
 - Constructed automated prompt-injection payloads to evaluate defensive safety guidelines of target agents in real-time.
 - Optimized multi-agent dialogue routing to surface logic loops, prompt drift, and sycophancy indicators.

Saksham Kapoor — Page 2/7

PAGE 3: AUDIO, SPEECH & MULTIMODAL AI

Vertical Focus: Speaker Diarization · Real-Time Voice Streaming · Multimodal ASR + Sentiment

Engineering high-fidelity, low-latency audio processing pipelines — from contact-center telephony and live voice proxying to academic multimodal sentiment extraction across 100+ dyadic sessions.

SPECIALLY FEATURED TOOLKIT

- *Go (Golang), WebSockets, WhisperX, pyannote.audio, Twilio SIP/RTP, G.711 PCMU, Gemini 1.5 Flash Native API, Docker, GCP Cloud Run*

COMPONENT PROJECTS

1. Gemini-Live-Go · Native Streaming Voice Proxy

- **The Innovation:** Bypasses legacy "Sandwich" pipeline latencies (Whisper STT → LLM → ElevenLabs TTS) by proxying real-time audio streams directly to Gemini 1.5 Flash's Native Multimodal Audio API.
- **Key Achievements:**
 - Developed a high-throughput Golang WebSocket server handling G.711 PCMU audio packet streams at sub-500ms end-to-end conversation latency.
 - Designed responsive barge-in controls enabling natural user interruption without robotic cutoff lag.

2. Voice-AI · Hexagonal Contact Center AI (CCAI) Engine

- **The Innovation:** A highly modular, hexagonal Go server for telephony stream processing with active agent coaching features at sub-800ms latency.
- **Key Achievements:**
 - Integrated Twilio SIP/RTP audio streams with parallelized STT and TTS synthesis models at sub-800ms latencies.
 - Deployed automated infrastructure pipelines using Docker and GCP Cloud Run for zero-downtime scaling.

3. MCD-NLP-PIPELINE · Multimodal Child Development NLP Pipeline (*UMD Research*)

- **The Innovation:** A production research pipeline automating speech processing and sentiment extraction across 100+ longitudinal parent-child study sessions.
- **Key Achievements:**
 - Coordinated end-to-end FFmpeg audio segmentation, WhisperX ASR transcription, and pyannote.audio speaker diarization.
 - Fine-tuned **RoBERTa** sentiment models integrated with Linear Mixed Effects Models in R to quantify emotional contagion.

Saksham Kapoor — Page 3/7

PAGE 4: REAL-TIME STREAMING & HIGH-PERFORMANCE SYSTEMS

Vertical Focus: Low-Latency Networking · High-Throughput Orchestration · DevTools & Observability

Building distributed systems operating at extreme throughput — from petabyte-scale AI agent observability platforms to event-driven supply chain microservices with guaranteed Saga consistency.

SPECIALLY FEATURED TOOLKIT

- *Go (Golang), NATS JetStream, ClickHouse, Spring Boot (Java), AWS SQS + DynamoDB, Raft Consensus, Docker, Kubernetes*

COMPONENT PROJECTS

1. PrismTrace · Universal AI Agent Observability Platform (*DevTools & Ops*)

- **The Innovation:** A Datadog-style tracing platform engineered to visualize multi-agent call trees, token costs, and latency hotspots across complex agentic workflows.
- **Key Achievements:**
 - Built a high-velocity Go ingestion API streaming agent trace metadata at **50,000+ operations/sec.**
 - Designed optimized ClickHouse schema tables supporting petabyte-scale long-term trace analytics with sub-second query latency.

2. AuraFlow · Event-Driven Supply Chain Intelligence

- **The Innovation:** A highly resilient microservices cluster utilizing the Saga pattern to guarantee strict transactional consistency across distributed logistics operations.
- **Key Achievements:**
 - Benchmarked Spring Boot services routing via AWS SQS and DynamoDB at **40,000 events/minute**.
 - Designed idempotency layers and compensating transaction handlers for multi-step order-to-fulfillment flows.

3. git-brain · AI-Powered Code Review Agent (*DevTools & Ops*)

- **The Innovation:** A Git-native intelligent PR review agent that summarizes diffs, surfaces anti-patterns, and posts structured multi-file feedback directly to GitHub.
- **Key Achievements:**
 - Built an automated pipeline fetching PR diffs via GitHub API and routing them through an LLM reasoning chain.
 - Integrated Playwright-based automated browser testing for CI/CD diff validation.

Saksham Kapoor — Page 4/7

PAGE 5: SCIENTIFIC MODELING, GIS & CAUSAL INFERENCE

Vertical Focus: Physics-Grounded ML · Structural Causal Models · Spatial-Temporal Systems

Leveraging advanced spatial-temporal GIS pipelines, agent-based terrain simulations, and structural causal models to solve high-impact academic and real-world societal problems — from disaster response to grid reliability.

SPECIALLY FEATURED TOOLKIT

- *Sentinel-1 SAR, DoWhy, GeoPandas, Mesa (ABM), Pyro, NetworkX, pandapower, SciPy, lifelines, PyTorch Normalizing Flows*

COMPONENT PROJECTS

1. CausalFlow · Causal Inference & Normalizing Flows Library

- **The Innovation:** A PyTorch library fusing Structural Equation Modeling (SEM) with Normalizing Flows for exact density estimation, causal discovery, and counterfactual query generation.
- **Key Achievements:**
 - Modeled structural causal equations using affine coupling layers to map arbitrary non-linear variables to Gaussian noise.

- Developed a counterfactual engine calculating interventions via forward/reverse coupling transformations.
- Evaluated DAG structures using NetworkX, DoWhy, and flow-based Jacobian determinants.

2. GridCert · Satellite-Enabled Utility & Grid Hardening Platform (*Security & Infosec*)

- **The Innovation:** A high-moat geospatial framework modeling physical power grid topology vulnerabilities against satellite remote-sensing indicators.
- **Key Achievements:**
 - Engineered Sentinel-1 SAR radar imagery pipelines to automatically detect vegetation encroachment hazards.
 - Designed topological grid contingency simulations in **pandapower** and NetworkX to forecast SAIDI/SAIFI reliability indices.
 - Generated localized risk-hardening maps using Mapbox GL JS and SciPy time-series decomposition.

3. nsri-72h-research · Search & Rescue (SAR) Agent-Based Simulation

- **The Innovation:** An analytical GIS simulation modeling lost person movement vectors within the critical first 72-hour SAR window.
- **Key Achievements:**
 - Programmed agent-based simulations using Mesa overlaying topological elevation grids and real-time weather layers.
 - Developed time-decay survival probability functions using GeoPandas, GDAL, and localized temperature grids.

4. TrialLens · Clinical Trial Cohort Analytics (*Healthcare*)

- **The Innovation:** A trial optimization system forecasting recruitment timelines and dropout risks using survival analysis.
- **Key Achievements:**
 - Integrated **lifelines** survival analysis libraries on synthesized clinical patient record datasets.
 - Built cohort stratification dashboards enabling early identification of at-risk patient subgroups.

Saksham Kapoor — Page 5/7

PAGE 6: CRYPTOGRAPHY, COMPLIANCE & B2B STARTUPS

Vertical Focus: Zero-Trust Ledgers · Automated Legal/Security Audits · HIPAA & SOC2

Building enterprise-grade tools that automate compliance auditing (HIPAA, SOC2, Legal contracts), establish zero-trust record custody on decentralized ledgers, and eliminate high-ticket billing disputes — across Healthcare and FinTech verticals.

SPECIALLY FEATURED TOOLKIT

- *Solidity, Polygon L2, Arweave, Open Policy Agent (Rego), Weaviate, AWS Textract, python-docx, CUAD-BERT, HIPAA BAA, pdflatex*
-

COMPONENT PROJECTS

1. VeriLedger · Immutable Multi-Tenant Cryptographic Ledger (*FinTech & Security*)

- **The Innovation:** A cryptographic record system eliminating transactional billing disputes by hashing operational states and securing them on decentralized permanent storage.
- **Key Achievements:**
 - Engineered deterministic SHA-256 state hashing to establish tamper-evident execution histories.
 - Wrote automated milestone verification smart contracts in Solidity deployed on Polygon L2.
 - Integrated the **Arweave** permanent ledger via the Irys SDK to secure multi-tenant execution logs immutably.

2. ClauseAudit · Legal Document Analysis & Tracked-Changes Engine (*FinTech & Legal*)

- **The Innovation:** An automated legal ops assistant flagging missing protective terms and drafting tracked-change replacements directly in Microsoft Word documents.
- **Key Achievements:**
 - Fine-tuned a CUAD-dataset BERT model to classify high-risk terms in corporate MSAs.
 - Built a python-docx tracked-changes injector overlaying visual contract risk heatmaps on raw `.docx` files.
 - Designed Weaviate-powered vector RAG matching clauses against thousands of legal clause templates.

3. MedLlama · Automated Pediatric Behavioral Clinical Suite (*Healthcare*)

- **The Innovation:** A fully audited, HIPAA-compliant platform automating behavioral annotation and drafting ICH E3 Clinical Study Reports (CSR) for pediatric research.
- **Key Achievements:**
 - Outlined AWS VPC secure isolation boundaries, PHI encryption via KMS, and Supabase HIPAA BAA integration.
 - Integrated the **TrustGen** SecOps engine to continuously audit and flag active HIPAA control drift in real-time.

4. TrustGen · Continuous Compliance & Evidence Auditing (*Security & Infosec*)

- **The Innovation:** A security dashboard executing Open Policy Agent (OPA) Rego rules to continuously audit AWS cloud environments for HIPAA and SOC2 drift.
 - **Key Achievements:**
 - Automated HIPAA/SOC2 compliance evidence report generation using pdflatex compiling from structured JSON evidence bundles.
-

PAGE 7: INTERACTIVE HCI, IMMERSIVE 3D & GENERATIVE UI

Vertical Focus: WebGL Engineering · Cognitive Psychology UX · Immersive & Gaming

Merging cognitive science principles with cutting-edge WebGL/Three.js graphics to create immersive, psychologically-informed digital interfaces that feel alive — from sentiment-reactive 3D orbs to psychology-backed e-commerce flows.

SPECIALLY FEATURED TOOLKIT

- *React Three Fiber (R3F), Three.js (WebGL), Framer Motion, Next.js 14, TypeScript, Tailwind CSS, Recharts, WCAG 2.1, Lexical Sentiment Analysis*
-

COMPONENT PROJECTS

1. AuraWeaver · 3D WebGL Ambient Sentiment Orb (*Immersive & Gaming*)

- **The Innovation:** A 3D ambient journaling platform that translates user writing sentiment into a live-morphing WebGL orb, making emotional states visually tangible.
- **Key Achievements:**
 - Programmed a Three.js/R3F 3D orb that morphs its shape, noise, and vertex colors in real-time based on compound sentiment scores.
 - Mapped lexical sentiment scores to coordinate deformation variables on the 3D mesh geometry.
 - Optimized rendering pipelines with custom memoizations guaranteeing stable **60fps** render cycles on consumer devices.

2. Tempo · Scroll-Driven Wellness Rhythm Planner (*Immersive & E-Commerce*)

- **The Innovation:** A time-management dashboard that transforms calendars into a peaceful, scroll-driven meditative storytelling experience.
- **Key Achievements:**
 - Developed scroll-linked Framer Motion timelines and a 3D parallax hero section with orbital animations.
 - Designed Recharts analytics visualizing user energy patterns against localized stress metrics.
 - Validated SOTA frontend performance targets: First Contentful Paint < 1.5s, TTI < 3s.

3. CogniCart · Psychology-Backed E-Commerce Platform (*E-Commerce*)

- **The Innovation:** An intelligent cart system that reflows product layouts based on the buyer's decision-making psychology style (analytical grid vs. intuitive flow).
- **Key Achievements:**
 - Structured dense comparison grids and custom keyboard shortcuts to maximize conversion speed for analytical buyers.

- Maintained strict accessibility compliance with WCAG 2.1 AA keyboard navigation and screen-reader support.

4. Saksham Innovation Lab · Personal R&D Portfolio Portal (*HCI & DevTools*)

- **The Innovation:** A curated, interactive portfolio hub demonstrating experimental R&D projects with live demos, structured project cards, and animated transitions.
- **Key Achievements:**
 - Architected a Next.js 14 multi-project portal with animated routing and cohesive design system.
 - Integrated live project status indicators and categorized filtering by research vertical.