

FEATURED PROJECT · ONE-PAGE SUMMARY

FraudShield V3: Real-Time Anomaly & Exception Detection

An anomalous transaction and an anomalous shipment are the same problem shape. FraudShield is a multi-release, production-style anomaly detection platform designed, architected, and built end-to-end, proven on payment fraud: the fastest, most adversarial version of the exception-triage problem every operations team faces.

Role: Technical Product Owner · System Architect · Lead Developer

Stack: Python · FastAPI · XGBoost · Isolation Forest · SHAP · GCP (Pub/Sub, Dataflow, Vertex AI, Feature Store, BigQuery) · Terraform

Status: V3 implemented · V4 roadmap defined **Code:** github.com/burnsgregm/fraudshield-v3

WHAT IT IS

A deliberately phased platform built across three releases: V1 baseline classifier and feature engineering; V2 full lifecycle with SHAP explanations, drift monitoring, and automated retraining; V3 real-time streaming features, a hybrid ensemble, and schema-level multi-tenancy.

KEY CAPABILITIES

- **Streaming features:** Pub/Sub ingestion into a Dataflow pipeline with event-time semantics (10-minute sliding windows, 1-minute advance), written to Vertex AI Feature Store.
- **Hybrid model:** XGBoost (supervised) plus Isolation Forest (unsupervised) combined in a custom prediction routine into a single score.
- **Online scoring API:** FastAPI fetches live features, calls the hybrid endpoint, returns score, component scores, and SHAP metadata.
- **Explainable by design:** SHAP built into the scoring path so an analyst can audit why an event was flagged.
- **Production discipline:** drift monitoring, automated retraining, and Terraform-defined infrastructure end to end.
- **Multi-tenant:** schema-level isolation with tenant_id on all entities.

MEASURED RESULTS

≈30%↓

False positives, V2 vs V1

90-180ms

End-to-end scoring latency

≤60s

Streaming feature freshness

Multi-tenant

Schema-level isolation

BUSINESS IMPACT

The same architecture that scores a suspect transaction scores a suspect shipment, work order, or supply event: real-time exception detection for operations, with fintech and payments as the proving-ground example. Deployment, evaluation, monitoring, and production-readiness in one system.