TEAM HACKERS

G.SAISHANKAR
N.YASHWANTH
M.SAISRIHITHA

Problem statement and define scope of your innovation

Problem statement : Develop AI solutions to enhance marketplace trust through advanced fraud detection, counterfeit prevention, and review authenticity verification. Use LLMs to analyze patterns in ratings, reviews and product listings to protect customer trust. Include real-time monitoring of product lifecycle from listing to returns.

Our Innovation : To address growing distrust and losses in online marketplaces, we propose an AI-powered "Trust Triad" system that ensures end-to-end marketplace integrity. This includes real-time fraud detection using behavioral analytics, counterfeit prevention through AI-powered image and metadata analysis, and review authenticity verification using LLMs to detect fake or incentivized content. Our solution offers full lifecycle monitoring — from product listing to transaction and returns — to rebuild customer confidence and protect platform reputation.

Working backwards from customer and define who is your customer

Title: Customer-Centric Trust Architecture

1. **Key Customer Segments & AI Solutions**

Segment	Key Pain Point	Our AI Solution
Shoppers	Counterfeit products	✓ Verified "Authentic" Badges
Brands	IP theft & fake listings	🔗 Blockchain provenance tracking
Sellers	Fraudulent competition	⚡ AI-powered violation alerts

2. How It Works

"A shopper searches for an iPhone → AI scans seller history → Blocks high-risk listings → Recommends trusted sellers"

SUCCESS METRICS & BUSINESS IMPACT

Quantifiable Trust Transformation

KPI	BASELINE	TARGET
FAKE LISTINGS	12%	↓ 60%
FRAUD TRANSACTIONS	8.5%	↓ 45%
REVIEW TRUST	58%	↑ 90%

- **Financial Impact:**
- "$2.1M saved daily"
- "18% conversion lift from trusted reviews"

SCALABILITY & EXPANSION

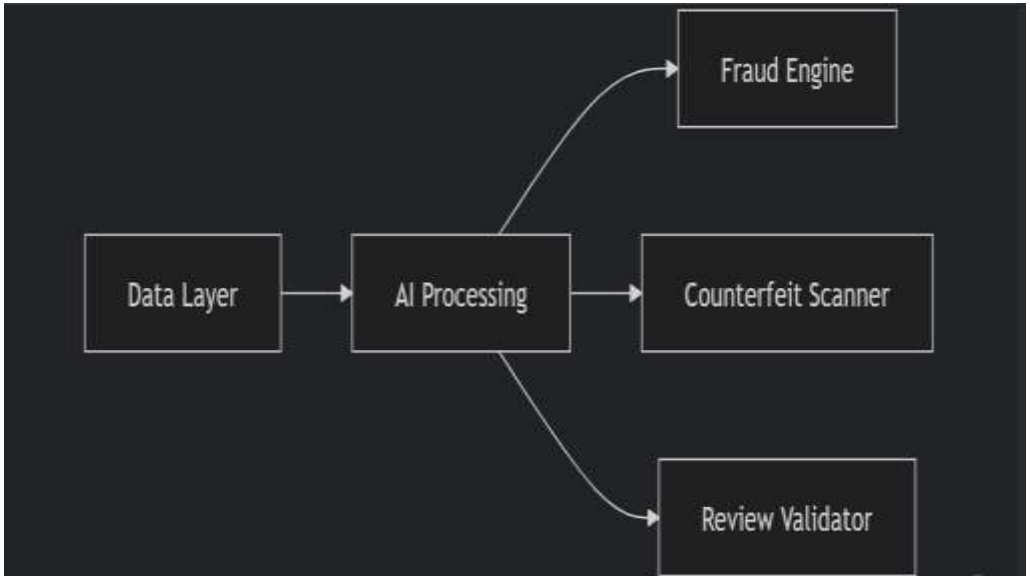
SCALABILITY LEVERS:

Our solution is built for scale using **AWS Kinesis** to handle up to **2 million transactions per second**, ensuring real-time fraud analytics. To make AI more cost-efficient, we leverage lightweight models like **DistilBERT**, achieving up to **90% reduction in inference costs** without compromising accuracy. Threat intelligence is geo-adaptive, with **localized detection mechanisms** to identify region-specific scams — such as Southeast Asia's rising gift card fraud trends.

DOMAIN EXPANSION ROADMAP:

We aim to deploy the Trust Triad in high-risk categories in a phased manner:
Phase 1 – Electronics (Q4 2024): Launch in top categories prone to counterfeits and high return rates.
Phase 2 – Luxury & Cosmetics (Q1 2025): Expand to brand-sensitive sectors requiring strong authenticity controls.
Phase 3 – Physical Retail (Mid 2025): Integrate with **Amazon Go** stores to detect product tampering and fraud at checkout using vision and sensor data.

ARCHITECTURE



Performance

- 92% decisions fully automated
- 8% escalated to human moderators
- 60% faster than legacy systems

TECH STACK

Layer	Technology	Function
Data Ingestion	AWS Kinesis, Apache Kafka	2M TPS real-time streaming
AI Processing	SageMaker, PyTorch	Multi-model inference orchestration
Fraud Engine	XGBoost, GNNs	Real-time transaction scoring
CV Scanner	Siamese Networks, ResNet-50	Image similarity detection (99.2% acc)
NLP Analysis	DistilBERT, RoBERTa	Review authenticity scoring
Storage	S3, Quantum Ledger DB	Immutable evidence logging