Tushin Kulshreshtha
San Francisco, California 94132
+1 (925) 819-4160 tushink04@gmail.com dextron04.in

Summary

Software Engineer with 4+ years building resilient distributed systems and security-focused platforms serving millions of users. Expertise in real-time anomaly detection, risk scoring engines, and fraud prevention systems. Proven track record implementing high-throughput architectures with 99.9%+ uptime, advanced machine learning for abuse detection, and scalable enforcement mechanisms. Strong background in fintech security, threat modeling, and zero-to-one system design.

Experience

SellWizr **June 2025 – Present**
Software Engineer Intern *New York, NY*

- Engineered Docker-based microservices infrastructure for enterprise CRM backend in Golang serving 10K+ users, implementing containerization patterns with real-time monitoring and threat detection that reduced security incidents by 40%.
- Designed and developed complex AI workflow system using Golang backend with anomaly detection pipelines and machine learning algorithms, improving fraud detection accuracy by 60% through distributed system architecture and real-time enforcement mechanisms.
- Implemented comprehensive observability and reliability standards in Golang microservices achieving 98% system availability, with rapid response capabilities for security incidents and automated threat mitigation reducing response time by 70%.

Site Service Software **Aug 2024 – Apr 2025**
Software Engineer Intern (Full Stack) *San Francisco, USA*

- Spearheaded migration of legacy payment systems to secure React/Spring Boot/PostgreSQL stack, implementing defense-in-depth security principles and OAuth 2.0 authentication reducing vulnerabilities by 85%.
- Developed 20+ RESTful APIs with comprehensive risk validation and threat modeling, implementing real-time fraud detection mechanisms and optimizing high-throughput database queries for sub-100ms response times.
- Built robust security monitoring system with JWT management and OWASP-compliant enforcement, creating resilient distributed architecture capable of handling 10K+ concurrent fraud detection requests.

MeetX **Feb 2025 – Apr 2025**
AI/ML Engineer *Bengaluru, India*

- Architected production-ready machine learning fraud detection system using advanced algorithms, achieving 95% accuracy in anomaly detection for 50K+ concurrent users through sophisticated risk scoring engines and real-time enforcement.
- Implemented deep learning-based abuse detection algorithms with real-time anomaly detection pipelines, reducing false positives by 40% and improving threat response times by 25% through distributed ML inference systems.
- Optimized high-performance ML models for fraud prevention using distributed computing frameworks, achieving 60% faster threat detection through scalable risk assessment systems and real-time monitoring infrastructure.

Glitter Fund **Jan 2023 – Dec 2023**
Lead Software Developer Intern *San Francisco, USA*

- Led team of 3 engineers building secure financial platform with real-time fraud monitoring, integrating trading APIs with advanced risk scoring systems and maintaining 99.9% uptime under adversarial conditions.
- Engineered custom risk assessment algorithms for financial fraud detection deployed on AWS with high-availability architecture, implementing real-time enforcement mechanisms and comprehensive threat monitoring systems.
- Implemented Redis-based caching and PostgreSQL optimization for high-throughput fraud detection, improving platform response times by 45% under attack scenarios through distributed security architecture and rapid response protocols.

Projects

Dex Pay - UPI Payment System with Fraud Detection (Next.js, PostgreSQL, TypeScript)

- Built comprehensive UPI-based payment platform replicating India's digital payment infrastructure with real-time fraud detection, implementing multi-layered security architecture with transaction monitoring and risk scoring engines for financial fraud prevention.
- Developed secure payment processing system with Virtual Payment Address (VPA) management and QR code authentication, featuring real-time enforcement mechanisms and comprehensive threat modeling for banking integration and fraud mitigation at scale.
- Implemented advanced authentication systems with risk-based transaction validation using PostgreSQL optimization and Tailwind CSS frontend, demonstrating expertise in adversarial fintech system design and defense-in-depth payment security principles.

AI-Powered Fraud Detection Platform (Python, Machine Learning, NLP)

- Engineered automated threat detection system using Python, spaCy NLP, and scikit-learn for intelligent fraud pattern recognition, implementing TF-IDF vectorization and cosine similarity algorithms for real-time anomaly detection and risk assessment.
- Built distributed fraud prevention pipeline with Selenium-based data collection and Google Gemini LLM analysis, featuring advanced behavioral pattern recognition and automated enforcement mechanisms for evolving attack vector detection.
- Developed comprehensive risk scoring engine processing 100K+ security events with pandas and numpy optimization, achieving 95% fraud detection accuracy through sophisticated ML models and real-time threat intelligence integration.

SafeWalk - Real-Time Threat Monitoring Platform (React, Node.js, WebSocket)

- Architected high-availability safety platform with real-time 911 data integration and threat detection using React, Node.js, and WebSocket, implementing intelligent route scoring algorithms and distributed alert systems for community-driven fraud prevention.
- Built resilient distributed architecture with Google Maps API integration and Leaflet visualization, featuring advanced threat modeling and anomaly detection capabilities for large-scale security monitoring and rapid incident response systems.
- Implemented comprehensive security observability with Chart.js analytics and automated threat response using Express backend, demonstrating expertise in building fault-tolerant systems under adversarial conditions with sub-second detection latency.

Education

San Francisco State University **Fall 2025**
Bachelor of Science in Computer Science — GPA: 3.95 — Phi Beta Kappa Honor Society *San Francisco, California*

Relevant Coursework: Distributed Systems, Computer Security, Machine Learning, Database Systems, Software Engineering, Computer Networks, Algorithms

Skills

Programming Languages: Golang, Python, JavaScript, Java, C, C++, SQL, Bash
Security & Fraud: Fraud Detection, Anomaly Detection, Risk Scoring, Threat Modeling, OAuth 2.0, OWASP
Distributed Systems: PostgreSQL, Redis, Kafka, Microservices, High-throughput Architecture, Real-time Processing
Machine Learning: TensorFlow, PyTorch, Scikit-learn, NLP, Behavioral Analysis, Pattern Recognition