CrowdZeroTrust: A Federated AI Approach to Zero Trust Security

Joseph Finnigan

University College London
Financial Technology MSc
In collaboration with NetraScale

September 2025

The Growing Threat

- $40 billion projected fraud losses by 2027
- Fraud has tripled since 2011
- AI-powered attacks increasing 30% annually

The Privacy Dilemma

- Banks need to share intelligence
- GDPR prevents data sharing
- Customer trust at stake
- Each bank fights alone

Traditional approach: Security OR Privacy

Our approach: Security AND Privacy

CrowdZeroTrust Solution

The Architecture

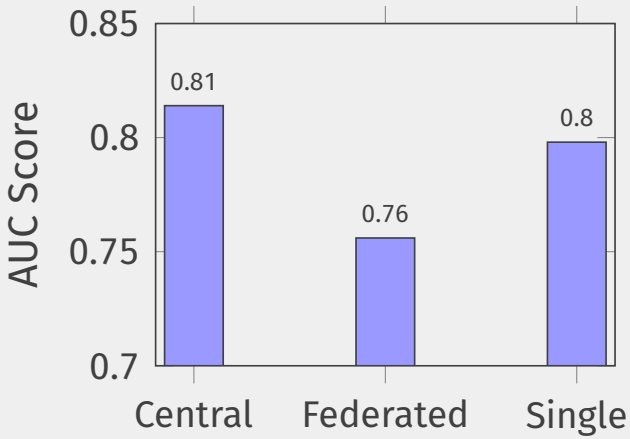
5 Banks
↓
Local Training
↓
Share Updates Only
↓
Central Aggregation
↓
Enhanced Model

How It Works

1. Train locally on own data
2. Share model updates only
3. Server combines learnings
4. Distribute improved model

Result: Learn from everyone, share with no one

Technical Implementation & Results



Our Approach

- NVIDIA FLARE
- XGBoost models
- 5 simulated banks
- 10,000+ transactions
- Zero data sharing

Key Achievement

93% performance retained with complete privacy

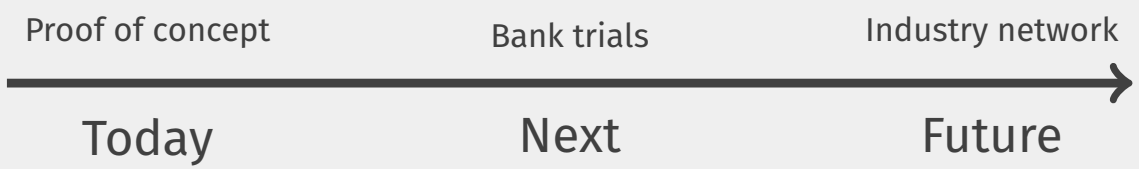
Impact & Future Vision

Immediate Benefits

- GDPR compliant
- No data breaches
- Customer trust maintained
- No single point of failure

Broader Applications

- **Healthcare:** Collaborative diagnosis
- **Cybersecurity:** Threat detection
- **Smart Cities:** Traffic optimization



Privacy-preserving collaborative AI is not just feasible - it's essential for the future of financial security