PSBs Hackathon Series-2025

(An initiative of Government of India, Ministry of Finance, Department of Financial Services)

Department of Financial Services
Ministry of Finance
Government of India

IDEA

INNOVATION | DEVELOPMENT | EXECUTION | ADVANCEMENT

SOMAIYA
VIDYAVIHAR UNIVERSITY

Promoting Innovation and Fostering Collaboration

PRESENTED BY

यूनियन बैंक
ऑफ इंडिया
Union Bank
of India

In association with K J Somaiya School of Engineering, Vidyavihar, Mumbai

EUCLID

SOCH SE
SACH TAK
Taking dreams of your journey to a defining reality

Problem Statement and Team Details

Team name (As submitted on portal)	
Domain	Generative AI
Problem Statement Title	Leveraging GenAI for Customer Analytics and Fraud Detection in Banking

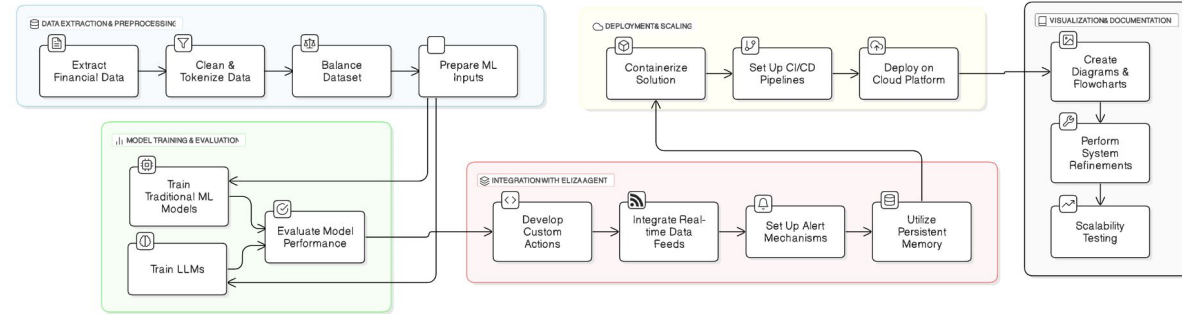|	Name	Area of Expertise
Member I (Team Leader)	Reeba Patel	UI/UX - Frontend
Member II	Shivankur Chavan	Backend
Member III	Savio Dias	GenAI
Member IV	Samuel Rodrigues	DevOps
Name of College	Agnel Charities' Fr. C. Rodrigues Institute of Technology, Vashi	

IDEA TITLE

Proposed Solution

- Our solution leverages generative AI and LLMs (e.g., FinBERT, GPT-2) integrated within the Eliza autonomous agent framework to enhance digital banking security and customer service. Key components include:

- 1. AI-Powered Risk Assessment & Customer Profiling

- 2. Real-Time Anomaly & Fraud Detection

- 3. Cross-Border Transaction Monitoring

- 4. Predictive Monitoring of Fraudulent Accounts

- 5. Insider Threat Detection

- 6. Personalized Customer Services

वित्तीय सेवाएं विभाग
DEPARTMENT OF
FINANCIAL SERVICES

यूनियन बैंक
ऑफ इंडिया
भारत सरकार का उपक्रम

Union Bank
of India
A Government of India Undertaking

IDEA
INNOVATION | DEVELOPMENT | EXECUTION | ADVANCEMENT

TECHNICAL APPROACH

Technologies to be Used:

- -Languages: TypeScript/JavaScript (for Eliza OS), Python (for data processing and ML).

- -Frameworks/Libraries: Eliza OS, TensorFlow/PyTorch, Scikit-learn, FinBERT, GPT-2, Pandas, NumPy.

- -DevOps: Docker, GitHub Actions; deployment on cloud platforms (AWS/Azure/GCP).

- •

Digital Banking Fraud Detection Solution

Methodology and Process:

- 1. Data Extraction & Preprocessing: Collect and clean financial filings (SEC reports); tokenize and balance datasets.

- 2. Model Training & Evaluation: Train and compare traditional ML models and LLMs (FinBERT, GPT-2) using metrics like precision, recall, and F1-score.

- 3. Integration: Embed custom fraud detection and risk assessment actions into the Eliza OS framework for real-time monitoring.

- 4. Deployment: Containerize the solution with Docker, set up CI/CD with GitHub Actions, and deploy on a scalable cloud platform.

SOMAIYA
VIDYAVIHAR UNIVERSITY

EUCLID

FEASIBILITY AND VIABILITY

- Feasibility and Viability

  Leverages proven technologies (Eliza OS, FinBERT, GPT-2, TensorFlow/PyTorch) with established data pipelines and containerized deployment. Modular design enables easy integration and scaling.

- Challenges & Risks:

  Data quality issues, high false-positive rates, evolving fraud tactics, regulatory compliance, and cybersecurity concerns.

- Mitigation Strategies:

  Continuous model updates with synthetic data augmentation, rigorous testing, and robust security and compliance frameworks.

- Viability:

  With increasing digital banking and sophisticated fraud techniques, our solution addresses a critical market need by offering cost savings, enhanced security, and improved customer trust, ensuring high adoption potential.

IMPACT AND BENEFITS

- Potential impact on the target audience

Banks & Financial Institutions

- Stronger fraud prevention & lower false positives
- Compliance with AML & cross-border regulations
- Reduced operational costs & automated fraud detection

Security & Compliance Teams

- AI-driven fraud intelligence & insider threat detection
- Faster investigations & automated compliance reports

Customers

- Faster fraud alerts & fewer blocked transactions
- Personalized banking services & enhanced security
- Increased trust in digital banking

Law Enforcement & Regulators

- Real-time fraud tracking & stronger compliance
- Faster detection of money laundering networks

Benefits of the Solution

Social Benefits
- Protects customers from financial fraud & identity theft
- Builds trust in digital banking, especially in rural & remote areas

Economic Benefits
- Reduces fraud-related financial losses for banks & customers
- Lowers operational costs with automated fraud detection

Environmental Benefits
- Reduces paper-based fraud investigations with AI-powered digital tracking
- Encourages remote banking, reducing carbon footprint from physical bank visits

Regulatory & Legal Benefits
- Strengthens compliance with AML & cross-border regulations
- Helps law enforcement track and prevent financial crimes

BUSINESS MODEL

- Revenue Streams:
  Subscription-based licensing, transaction fees, and consulting services.

- Target Customers:
  Banks, fintech companies, and other financial institutions.

- Value Proposition:
  Improved fraud detection accuracy, reduced operational costs, streamlined compliance, and personalized customer services.

- Commercialization & Scalability:
  Cloud-based, scalable deployment; integration with existing banking systems; strategic partnerships with technology providers; and global market expansion opportunities.

RESEARCH AND REFERENCES

- 1. Eliza OS Repository
  URL: https://github.com/elizaOS/eliza

- 2. Financial Fraud Detection Using LLMs
  URL: https://github.com/amitkediaOO7/Financial-Fraud-Detection-Using-LLMs

- 3. LLMs in Banking Enhance Fraud Detection, Risk Assessment, and Credit Evaluation (PDI Blog)
  URL:
  https://www.pacificdataintegrators.com/blogs/llms-in-banking-enhance-fraud-detection-risk-assessment

- 4. Pacific Data Integrators Website
  URL: https://www.pacificdataintegrators.com

- Mandatory Submission:
  https://docs.google.com/document/d/1OjJKWcP8e_GQDCXpe-vJQEk6GtELfGQeyUDciNNqZ7k/edit?usp=sharing