

SEBI Verify: An AI-Powered Investor Shield Against Securities Fraud

Requirements Document

Document Version: 1.0

Date: July 20, 2025

1. Introduction

1.1 Problem Statement

The rapid digitization of financial services has unfortunately been accompanied by a surge in sophisticated securities fraud, severely impacting retail investors and eroding trust in capital markets. Fraudsters employ a wide array of deceptive tactics, including impersonating SEBI-registered entities, disseminating deepfake audio/video content of market influencers, orchestrating pump-and-dump schemes via social media (e.g., Telegram groups), luring investors with false promises of IPO allotments, and deploying malicious or fake trading applications. These activities lead to significant financial losses for individuals, create systemic risks, and pose considerable challenges for regulatory oversight. A proactive, accessible, and intelligent solution is urgently needed to empower investors and assist regulators.

1.2 Project Vision & Mission

- **Vision:** To foster a secure and transparent Indian securities market where every investor is protected from evolving fraudulent activities through readily available, intelligent verification and detection tools.
- **Mission:** To develop "SEBI Verify," an AI-powered mobile application that serves as a personal "Investor Shield," enabling retail investors to verify financial entities and offerings, detect potential scams across diverse digital content, and contribute to a safer investment ecosystem.

1.3 Target Audience

- **Primary:** Retail investors, particularly those new to the stock market or less technologically savvy.
- **Secondary:** SEBI and other financial regulators (as beneficiaries of aggregated intelligence and potential future integrations).

2. Solution Overview: SEBI Verify

2.1 Core Concept

"SEBI Verify" will be a user-friendly mobile application that acts as a frontline defense against various forms of securities fraud. It will initially provide essential verification services, then progressively integrate advanced AI capabilities (leveraging Google's Gemini 2.5 Pro and Vertex AI) to identify nuanced and sophisticated scam patterns across multimodal data. The app aims to empower investors by providing actionable insights and facilitate regulatory intelligence.

2.2 High-Level Architecture

The solution will primarily comprise:

- **Mobile Frontend:** Cross-platform application (e.g., React Native/Flutter) for user interaction.
- **Backend API Service:** (e.g., Flask/Node.js) handling business logic, data storage, and communication with AI services.
- **Data Layer:** Initially local mock data (JSON/SQLite), evolving to robust databases.
- **AI/ML Layer:** Google Cloud's Vertex AI for managing and deploying models, including calls to Gemini 2.5 Pro API.

3. Detailed Feature Requirements

Features are categorized into tiers based on priority for a hackathon environment.

3.1 Tier 1: Core MVP Features (Must-Haves)

These are essential for a strong, demonstrable prototype.

3.1.1 User Authentication (Optional but Recommended)

- **REQ-AUTH-001:** The system shall allow users to register with email/password.
- **REQ-AUTH-002:** The system shall allow registered users to log in securely.
- **REQ-AUTH-003:** (Future) Implement social login options (Google, Apple).

3.1.2 Advisor/Entity Verification

- **REQ-VERF-001:** The app shall provide a clear input field for users to enter the name or SEBI registration ID of a financial entity.
- **REQ-VERF-002:** The app shall query a backend database (initially simulated mock data) to verify the entity's registration status.
- **REQ-VERF-003:** The app shall display clear visual feedback:
 - **Green checkmark/indicator** for "Verified" with registered details (Name, ID, Type, Status).
 - **Red cross/indicator** for "Not Found" or "Not Registered."
- **REQ-VERF-004:** The app shall handle various query inputs (full name, partial

name, ID).

3.1.3 Suspicious URL/App Scanner

- **REQ-SCAN-001:** The app shall provide an input field for users to paste a suspicious URL or type an App name.
- **REQ-SCAN-002:** The app shall analyze the input against a pre-defined rule-set and a mock blacklist of scam indicators.
- **REQ-SCAN-003:** The app shall display clear visual feedback:
 - **Red flag/indicator** for "Potential Scam Detected" with a concise reason (e.g., "Promises unrealistic returns," "Known phishing pattern").
 - **Green checkmark/indicator** for "Looks Safe" (no obvious threats detected).
- **REQ-SCAN-004:** The analysis should include basic checks for URL irregularities and app name red flags.

3.1.4 User Interface (UI) & User Experience (UX)

- **REQ-UIX-001:** The app shall have a clean, intuitive, and simple design.
- **REQ-UIX-002:** The app shall provide clear instructions and concise error/success messages.
- **REQ-UIX-003:** The app shall offer easy navigation between different core functionalities.
- **REQ-UIX-004:** The visual aesthetics shall inspire trust and professionalism.

3.2 Tier 2: Stretch Features (Nice-to-Haves)

These enhance functionality and differentiate the solution.

- **REQ-CONT-001:** Allow users to paste blocks of text for analysis.
- **REQ-CONT-002:** Use basic NLP to flag common scam phrases.
- **REQ-CONT-003:** Perform basic domain authenticity checks on URLs.
- **REQ-REPT-001:** Provide a "Report a Scam" feature.
- **REQ-REPT-002:** Store submitted reports in the backend.
- **REQ-EDU-001:** Display concise educational tips about common scams.

3.3 Tier 3: Future Vision Features (Long-Term Potential)

These demonstrate the solution's scalability and long-term impact.

- **REQ-PRED-001:** Utilize Gemini 2.5 Pro to analyze OSINT data to predict emerging fraud.
- **REQ-MMCV-001:** Integrate AI models for deepfake audio/video detection.
- **REQ-MMCV-002:** Implement forensic analysis of scanned documents.
- **REQ-GAME-001:** Provide interactive, personalized learning modules.
- **REQ-REG-001:** Develop a real-time AI dashboard for regulators.

- **REQ-REPT-003:** Enhance scam reporting with AI-powered processing.
- **REQ-USER-001:** Allow users to create watchlists for proactive alerts.

4. AI Integration: Leveraging Gemini 2.5 Pro & Vertex AI

4.1 Gemini 2.5 Pro Capabilities & Application

- **Multimodal Analysis:** Process text, images, audio, and video to understand complex scams.
- **Contextual Understanding:** Analyze extensive conversations to discern subtle manipulation tactics.
- **Cross-Modal Correlation:** Connect disparate pieces of information to build a comprehensive fraud profile.
- **Generative Capabilities:** Generate clear summaries of threats and educational content.

4.2 Vertex AI for MLOps & Scalability

- **Model Training & Fine-tuning:** Fine-tune Gemini 2.5 Pro with Indian market-specific fraud data.
- **Model Deployment & Serving:** Deploy models as scalable APIs for real-time app queries.
- **Continuous Monitoring & Improvement:** Monitor model performance and orchestrate retraining to combat evolving threats.
- **Data Pipelines:** Manage secure data pipelines for continuous learning.
- **Explainable AI:** Provide rationale behind AI decisions for trust and compliance.

5. Addressing Specific Fraud Types

"SEBI Verify" is designed to combat:

- **Fraudulent Advisors/Ponzi Schemes**
- **Deepfakes/Fabricated Content**
- **Social Media Manipulation (e.g., Telegram Bots)**
- **Fake Intermediaries/IPO Allotment Scams**
- **Fake Trading Apps**

6. Technical Considerations

6.1 Recommended Tech Stack

- **Frontend:** React Native
- **Backend:** Python with Flask/FastAPI or Node.js with Express
- **Database:** JSON files/SQLite (initially), PostgreSQL/MongoDB (for scale)
- **Cloud Platform:** Google Cloud Platform (Vertex AI, Gemini APIs)

6.2 Data Requirements

- **Mock Data:** Simulated datasets for SEBI-registered entities, suspicious URLs, and scam phrases.
- **Real Data (Future):** Official SEBI registration data, reported scam databases, social media data, market data.

7. Project Success & Impact

7.1 Key Differentiators

- **Multimodal AI Power:** Advanced, contextual fraud understanding.
- **User-Centric Design:** Simplicity and immediate utility.
- **Scalable Architecture:** Built for continuous improvement.
- **Proactive Approach:** Warns investors *before* they become victims.

7.2 Expected Impact

- **Reduced Investor Losses**
- **Increased Market Trust**
- **Enhanced Regulatory Efficiency**
- **Improved Financial Literacy**

7.3 Hackathon Winning Strategy

Deliver a flawless MVP of the Advisor/Entity Verification and Suspicious URL/App Scanner. The pitch will demonstrate these core features and vividly present the future vision driven by Gemini 2.5 Pro and Vertex AI.