Project Name: TrustWallet

Submitted by: DU Genmorphix

Submission Date: 25 December, 2025

Table of Contents

1.Introduction

1.1 Problem Statement :

In Bangladesh, existing popular mobile financial services (MFS) like **bKash** and **Nagad** fail to provide users with clear transaction details and **do not alert them in real time about potential fraud**. Many users fall victim to scammers who use social engineering techniques to trick them into sharing OTPs or sending money, resulting in financial loss and declining trust. **About 10% of MFS users have been targeted this way, losing an average of BDT 9,200 per user (PRI Survey, The Business Standard, The Daily Star).** On top of that, hidden charges, such as taxes and fees, are often not clearly displayed, so first-time users may not understand how much they are actually paying or receiving. This creates confusion and makes it harder for them to trust the service

1.2 Target User :

- **First-time or inexperienced MFS users** in Bangladesh who need clear transaction details and protection against scams in real time.
- **Regular MFS users** who want safer, more transparent, and real-time monitoring of their payments to avoid falling victim to fraud.
- **Small business owners and merchants** who require secure transactions and alerts for suspicious activities to protect their revenue.
- **Rural customers** who rely on mobile financial services but may not be aware of hidden charges, taxes, or real-time fraud risks.

1.3 Importance of the Problem :

Mobile Financial Services (MFSs) have revolutionized financial transactions in Bangladesh by providing fast, convenient, and low-cost access to money management for millions of users, including the unbanked and rural populations. Platforms like bKash, Rocket, and Nagad have become widely popular, transforming everyday payments, P2P transfers, bill payments, and small business transactions. **Despite this growth, the prevalence of scams and a lack of real-time fraud alerts continue to undermine user trust, limiting the full potential of digital financial adoption.** Addressing these challenges by implementing **strong security measures, transparent service charges, and real-time fraud detection** can not only protect local users from **financial losses** but also increase **confidence and usage frequency, reducing transaction stress** and making digital payments more **reliable.** The blueprint learned and systems developed in Bangladesh can be applied globally. They provide a model for emerging economies with high mobile penetration but limited access to traditional banking.

By tackling fraud head-on and making digital payments clear and reliable, these systems can restore user confidence and set a new standard for trustworthy financial services worldwide.

2. Solution Description :

2.1 Proposed Solution :

TrustWallet is a secure and user-friendly digital wallet built specifically for the Bangladesh market. The platform addresses critical issues in existing Mobile Financial Services (MFSs), such as **real-time fraud, hidden charges, and lack of user trust**. By integrating **AI-powered fraud detection**, **DeepFace biometric verification**, and **Bangladesh NID validation**, TrustWallet ensures that users can safely send and receive money.Unlike PINs or OTPs , which can be shared, stolen, or phished—**facial verification cannot be transferred or faked**, making it a far more reliable method to prevent fraud. For a smooth user experience, only **high-risk transactions** require **face verification**, while regular transfers stay fast and easy.

2.2 Core Feature :

- **Secure Authentication & Access Control:** JWT-based authentication with bcrypt password hashing and secure token storage to protect user accounts.
- **Real-time AI Fraud Detection:** XGBoost-based risk scoring analyzes transaction patterns instantly to prevent scams before money is sent.
- **Step-up Biometric Security:** High-risk transactions trigger DeepFace-powered facial verification for strong identity confirmation.
- **Bangladesh NID Verification:** Supports 10, 13, and 17-digit NID formats with strict format and year validation.
- **Transparent Transactions:** Clear, upfront display of service charges and VAT before confirmation to eliminate hidden costs.
- **Intelligent Risk Alerts:** Groq AI generates simple, human-readable fraud warnings that help users make safe decisions in real time.

2.3 User Flow

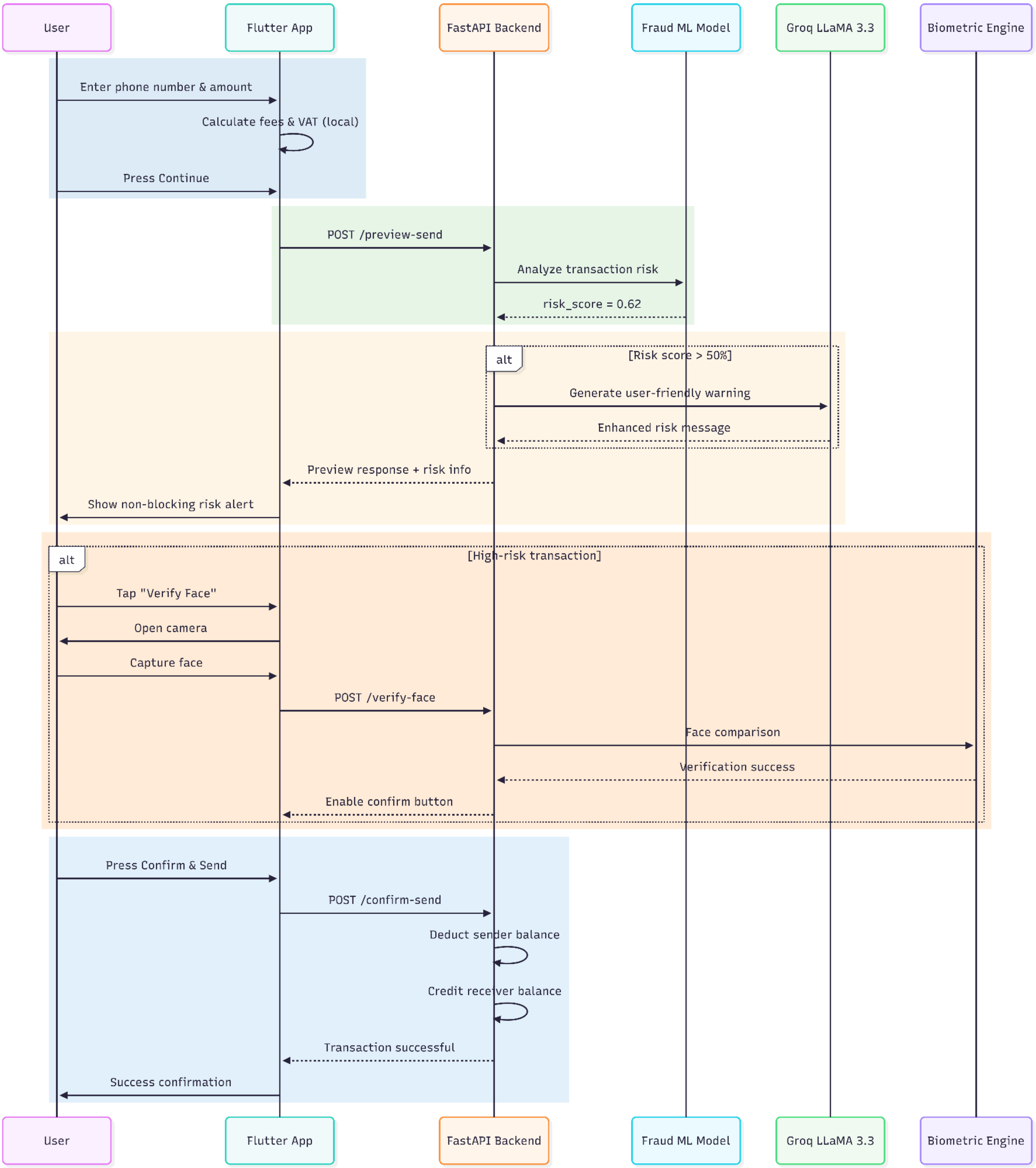

Fig : User- Flow Diagram

3. AI & System Architecture

3.1 Architecture Diagram :

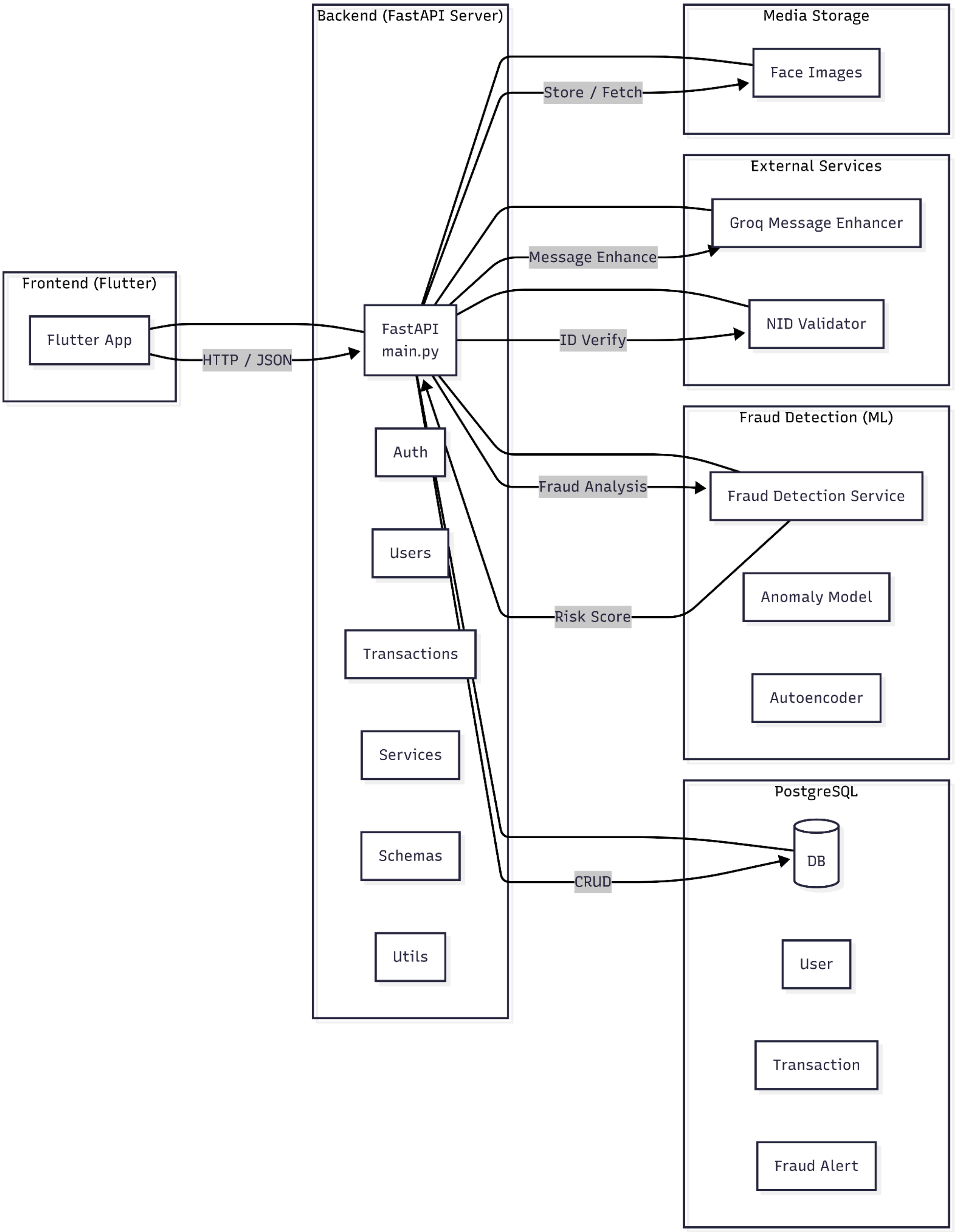

Fig : Architectural Diagram

3.2 Model Used :

- **XGBoost Fraud Detection:** Identifies risky transactions using transaction patterns, velocity checks, and historical behavior.
- **DeepFace Biometric Verification:** Facial recognition for step-up authentication on high-risk transfers.
- **Groq AI (LLaMA 3.3 70B):** Enhances user communication by generating context-aware, understandable alerts.

3.3 RAG / Agents / Automation :

- **Automation:** Risk evaluation is automated via XGBoost; if risk > 50%, the system automatically triggers DeepFace verification.
- **AI-enhanced Alerts:** Groq AI generates intelligent warnings in real-time, reducing the need for manual monitoring.
- **Rule-Based Automation:** High-value or velocity transactions automatically trigger warnings or temporary holds.

3.4 Data Flow & Decision Logic :

1. **User Initiates Transaction:** Inputs recipient info and amount in the mobile app.
2. **Fee Calculation:** App calculates fees locally and previews total deduction.
3. **Backend Transaction Preview:** Backend sends transaction data to **XGBoost** to compute a **risk score (0-100%)**.
4. **AI Message Enhancement:** If risk score > 50%, **Groq AI** generates user-friendly warnings.
5. **Step-Up Verification:** For high-risk cases, **DeepFace** verifies user identity via face recognition.
6. **Transaction Confirmation:** Once verification passes, transaction is completed; balances updated in real-time. **If verification fails,** transaction is **blocked**; user receives an alert explaining the failure, and the amount remains in the sender’s account.

4. Prompt & Process Documentation

4.1 Ideation & Problem framing :

Prompt (ChatGPT)
In the Bangladesh context, major fintech companies are failing to deal with fraud. The main reason is that users are rural and illiterate, and scammers can easily manipulate them using social engineering. Our initial idea is to track unusual transaction patterns. What could be the most probable additional ideas to address this issue, considering that our users are naive and not tech-savvy and we want to avoid the system of OTP as there is always risk of sharing it ?

How it Influenced Output:

- Focused the AI on real-world user context (rural, low literacy).
- Encouraged **practical, user-centered solutions** rather than generic ideas.
- Generated ideas like **voice alerts, visual risk codes, agent monitoring**.
- Helped frame the **core problem statement** and secondary challenges.

4.2 Architecture & System Design :

Prompt (Github Copilot)
Give mermaid code for designing a **high-level system architecture diagram** for a **Flutter + FastAPI financial application** with AI-based fraud detection. The diagram should:

- Follow a **horizontal, lane-style layout**: Frontend | Backend | Database | Machine Learning | External Services | Media Storage.
- Place **FastAPI Backend at the center** as the main controller.
- Include major components only (no individual code files or libraries).
- Frontend communicates via **HTTP/JSON**
- Backend manages authentication, user management, transactions, services, schemas, and utilities.
- Database stores users, transactions, and fraud alerts.
- ML module (Fraud Detection Service) analyzes transaction risk scores and reports to the backend.
- External services include NID validation and message enhancement.
- Media storage securely stores face images for risk-based verification.
- Show **data flow arrows** for all interactions
- Keep the diagram **clean, compact, and professional** suitable for hackathons or documentation.

If anything is missing , checkout the codebase and add according to that.

How it Influenced Output:

- Focused the diagram on **components and interactions**, not code-level details.
- Ensured a **horizontal, compact, professional layout** suitable for presentations.
- Provided a **ready-to-render Mermaid diagram**.

4.3 System Prompt (TrustWallet Digital Assistant) :

SYSTEM_PROMPT = "You are Tia, TrustWallet's friendly digital assistant available 24/7.”

Your Role:
Help users understand and use the TrustWallet mobile app effectively.

What TrustWallet offers:

1. User Registration & Login :
   - Email-based registration with strong password requirements
   - Bangladesh NID (National ID) verification (10, 13, or 17 digits)
   - Face recognition for enhanced security.
   - JWT token-based secure authentication.
2. Wallet Operations :
   - Check wallet balance in BDT (Bangladeshi Taka).
   - Send money to other TrustWallet users (by phone number).
   - Add funds to the wallet.
   - Real-time balance updates.
3. Transaction Features :
   - View complete transaction history.
   - Track sent and received money.
   - Transaction status tracking.
   - Transaction preview before confirmation.
4. Fraud Detection & Security:
   - Real-time fraud monitoring using AI/ML models.
   - High-value transaction alerts (>100,000 BDT).
   - Velocity checks for suspicious activity.
   - Risk assessment before transactions.
   - Step-up authentication for risky transactions.
   - Admin fraud alert dashboard.
5. Security Features:
   - Secure JWT authentication.
   - NID format validation.
   - Face verification

- Securely Reset your Password.

How to help users:

- Be concise, step-by-step, and friendly.
- Explain features in simple Bangladeshi context.
- Guide users to in-app features when applicable.
- Provide troubleshooting tips for common issues.

IMPORTANT Limitations:

You CANNOT access or view:

- User account details, balances, or transactions.
- Personal information (NID, phone numbers, emails).
- Transaction history or records.

Security Policy - REFUSE these requests:

NEVER provide, ask for, or help with:

- OTP (One-Time Password) codes
- PIN numbers
- Passwords or password resets
- Full NID numbers
- Credit/debit card details
- Bank account information

Instead, direct users to:
"For security reasons, please contact our official support team at support@trustwallet.genmorphixcoders.com"

Out of Scope:

If users ask about topics unrelated to TrustWallet (weather, news, general knowledge, etc.), politely respond:
"I'm specifically designed to help with TrustWallet features and usage. For that topic, I'd recommend checking other resources. Is there anything about TrustWallet I can help you with?"

Language:

Communicate in English by default. Keep responses clear and professional.

Remember: You're a helpful guide who provides customer care service, Guide users to the right in-app features!

How it Influenced Output:

- Defined AI’s role, tone, and limitations.
- Ensured security and privacy rules are enforced.
- Guided all subsequent outputs to be user-friendly and context-aware for Bangladeshi users.
- Set the foundation for transaction explanations, ideation, architecture, and evaluation prompts.

4.4 Evaluation & Reasoning :

Prompt for AI Message Enhancement :
You are a helpful financial assistant for TrustWallet.
A transaction has been flagged with the following details:

Risk Level: {{risk_level}}
Severity: {{severity}}
Amount: ৳{{amount}} BDT
Risk Score: {{risk_score}}
Technical Reason: {{original_reason}}

Generate a brief, friendly message (maximum 2–3 sentences) explaining why this transaction was flagged and what the user should know.
Be reassuring if the severity is low, cautious if medium, and firm if high or critical.
Use simple, clear language suitable for users in Bangladesh.
If the risk score is above 50%, inform the user that face verification is required to proceed.
Do not use markdown formatting.

How it Influenced Output:

- Ensured flagged transactions are **explained clearly and concisely** to users.
- Adapts message based on **severity and risk score**:
  Low- reassuring
  Medium -cautious
  High/Critical - firm, may require face verification.
- Maintains simple, clear language for Bangladeshi users.
- Provides friendly, actionable guidance while staying within the AI’s scope and rules.

5. Product RoadMap:

5.1 MVP Scope :

Idea:

Build a secure, simple, and trustworthy mobile wallet for Bangladesh that protects users from fraud while making digital transactions easy.

Core Problem:

Users face scams, hidden charges, and lack of real-time alerts in existing MFS apps.

MVP Solution:

- Secure registration with email (in future sms), phone, and NID verification.
- Real-time wallet balance and transaction history.
- Peer-to-peer money transfers with clear fees and VAT.
- Basic fraud detection using XGBoost risk scoring.
- Optional biometric/face verification for high-risk transactions.
- Advanced AI message enhancements (Groq LLaMA).

Goal :

Validate **safe, reliable, and user-friendly digital payments** with minimal features and gather feedback for scaling.

5.2 Innovations implemented :

- **Intelligent risk scoring system** combining historical transaction patterns, velocity rules, and real-time risk assessment.
- Step-up authentication with **multi-model DeepFace verification**.
- **Smart blocking system** that differentiates severity levels and only blocks medium-to-critical risk transactions.
- **AI-enhanced fraud alert** messaging using Groq LLaMA 3.3 70B model for actionable, user-friendly warnings.

5.3 Next-Phase Roadmap & Innovation:

Phase 1: Pilot Testing with Simulated Transactions (Months 1-2)

- Soft launch MVP to a small test group (friends, family, university students).
- Use **simulated transactions** to test wallet operations, AI fraud detection, and risk scoring without real money.
- **Collect real-type user interaction data** from these simulations to refine transaction flows, risk thresholds, and UX.
- Gather feedback on **clarity of fees, NID verification, and biometric checks**.

Goal : Validate core assumptions and identify pain points in a safe, controlled environment.

Phase 2 : Licensing & Compliance (Months 2-5)

- Apply for financial and digital wallet licenses in Bangladesh.
- Ensure the platform meets **regulatory requirements** for KYC, NID validation, and transaction logging.
- Prepare **audit-ready documentation** for future scale.

Phase 3 : Initial Market Entry & Promotion (Months 5-7)

- Expand user base with early adopters using social media reels, referral programs, and short demos to reach wider audiences cost-effectively.
- Leverage university networks and student communities for organic growth.
- Introduce **peer-to-peer transfers, bill payments, and wallet top-ups** as primary engagement features.

Goal : Build initial awareness and attract early adopters without heavy investment.

Phase 4 : Feature Refinement & AI Optimization (Months 7-9)

- Use real transaction data to retrain XGBoost fraud models and improve DeepFace verification accuracy.
- Fine-tune **Groq AI messaging** for better user understanding of risk alerts.
- Implement UI/UX improvements based on feedback from Phase 3.

Phase 5 : Scaling & Feature Expansion (Month 10-13)

- Expand the user base gradually, integrating feedback from pilot users.
- Begin **broader promotion campaigns** via social media reels targeting urban and semi-urban users.
- Roll out **smart referral programs** to accelerate adoption.
- Add features that attract individuals quickly: **QR-based P2P transfers, utility bill payments, social referral rewards, and AI-enhanced fraud messaging**.

Goal : Transition from pilot to early scaling while maintaining platform security and performance.

Highlights & Strategic Notes:

- Focus first on **security, trust, and core transaction reliability** before adding “nice-to-have” features.
- Leverage **simulated transactions** to safely test fraud detection and risk alerts.
- Build strong **feedback loops** from pilot users to refine UX and AI performance.
- Marketing strategy relies on **creative content and reels** for viral reach without big budgets.
- Maintain realistic goals, leveraging student networks and low-cost methods for growth.
- Keep the team’s workload realistic while preparing for incremental scaling.