Project Blueprint: ThreatLens - Fraudulent Link Detection App

1. Project Overview

ThreatLens is a cross-platform security application designed to help users identify and avoid fraudulent, malicious, or phishing URLs. It combines threat intelligence services, AI-based analysis, and intuitive user interfaces to protect users before they interact with harmful links.

2. Core Features

- Real-time Link Analysis
- Phishing and Scam Detection (via AI)
- Browser Extension for Instant Link Checks
- Educational Warnings & Security Tips
- User Feedback and Reporting System
- Dashboard with Link History and Risk Levels

3. System Architecture

Modules and Technologies:

- Frontend: React.js / Flutter
- Browser Extension: JavaScript (Manifest V3)
- Backend API: FastAPI (Python)
- ML Service: Python (Scikit-learn, TensorFlow)
- Database: PostgreSQL + Redis
- Cloud & DevOps: AWS / Docker / GitHub Actions
- Threat Intelligence: VirusTotal, Google Safe Browsing API

4. Folder Structure

ThreatLens/

client/

server/

ml_engine/

threat_intel/

browser_extension/

database/

docker/

.env

README.md

5. Development Phases and Timeline

Phase 1: Setup & Planning (1 week)

Phase 2: Core Backend & APIs (23 weeks)

Phase 3: Machine Learning Integration (23 weeks)

Phase 4: Frontend UI & Browser Extension (23 weeks)

Phase 5: Database & Logging (1 week)

Phase 6: Testing & Security (1 week)

Phase 7: Deployment & Documentation (1 week)

Estimated Total Duration: 812 weeks (with AI assistance)

6. Security Measures

- HTTPS + OAuth 2.0 Authentication

- Input sanitization & API rate limiting

- AES-256 encryption for sensitive data

- WAF & IDS on cloud infra

- Regular model retraining

7. Future Enhancements

- Auto-scanning of email and message links

- Advanced NLP content scanning on webpages

- Real-time threat alerts via notifications

- Integration with antivirus/browser software