OS-Level AI Phishing Detection System (Phased Implementation Plan)

Phase 1: Foundation & OS-Level Setup

Goal: Create a stable OS-level application skeleton.

1. Set up Python project structure
2. Create always-on-top floating widget (Protection ON/OFF)
3. Detect active window and application metadata
4. Implement background service loop

Phase 2: Screen Capture & Accessibility Integration

Goal: Acquire text from any running application.

1. Capture active window screenshots using MSS
2. Integrate Windows UI Automation for accessibility text
3. Handle window switches and content refresh

Phase 3: OCR & Text Extraction

Goal: Convert visual data into usable text.

1. Integrate EasyOCR for screen text extraction
2. Merge OCR text with accessibility text
3. Noise removal and duplicate filtering

Phase 4: Text Processing & Chunking

Goal: Prepare text for LLM analysis.

1. Clean UI artifacts and irrelevant tokens
2. Implement logical chunking (300–700 words)
3. Maintain rolling context for long documents

Phase 5: Groq LLM Integration

Goal: Perform intelligent phishing detection.

1. Integrate Groq API with secure key handling
2. Design phishing-detection prompts

3. Parse structured JSON responses

Phase 6: Decision Engine & Risk Scoring

Goal: Aggregate results and determine final alerts.

1. Combine results from multiple text chunks
2. Implement risk-level logic (Low/Medium/High)
3. Trigger alerts based on thresholds

Phase 7: UI Alerts & User Interaction

Goal: Notify users clearly and safely.

1. Update widget color/status dynamically
2. Show explanation and suspicious text
3. Allow user to pause or disable detection

Phase 8: Optimization, Security & Testing

Goal: Make the system robust and ethical.

1. Optimize OCR frequency and API calls
2. Ensure no data is stored permanently
3. Test across browsers, Notepad, PDFs, emails

Phase 9: Documentation & Presentation

Goal: Prepare for academic and interview evaluation.

1. Prepare final project report
2. Create architecture diagrams
3. Prepare demo and explanation flow