Antivirus: AI-Based Threat Detection

Functional Requirements

FR1. Directory-Based File Scanning
The system must accept a directory path and recursively scan all files within that directory and its subdirectories for potential malware.

FR2. Signature-Based Detection
The system must compare the file signature (or hash) against a local signature database of known malware signatures. If a match is found, the file is flagged as malicious.

FR3. AI-Enhanced Behavioral Analysis
For files not matched via signatures, the system must analyze file metadata (size, type, timestamps, entropy, etc.) using a lightweight AI module to predict whether a file is suspicious. The AI module is local and does not require internet access.

FR4. Malware Alerting
When malware or suspicious files are detected, the system must alert the user with clear messages in the UI (e.g., "⚠ ALERT: Malware detected at [file path]"). Optionally, a simple notification popup on Windows may be implemented.

FR5. Quarantine Management
Detected malware files should be moved to a secure quarantine folder with restricted access to prevent accidental execution.

FR6. Malware Removal
The user must be able to choose to permanently delete quarantined malware files from the system after confirmation.

FR7. Logging of Results
The system must generate logs of scan results including timestamps, file names, detection results, and actions taken. Logs must be stored locally.

FR8. Signature Database Management
The system must allow for manual signature database updates by the user, with clear logs indicating the last update time. Automatic updates are optional.

Non-Functional Requirements

NFR1. Performance
The scanner should be able to process hundreds of files in the efficient manner.

NFR2. Accuracy and Reliability
Very low false positive rate. Signature database and AI module must be reliable and validated with known samples.

NFR3. Usability
Clear and simple UI with easy-to-understand outputs. Users with basic technical knowledge should be able to operate the scanner.

NFR4. Maintainability and Modularity
Codebase must be modular with separate components for scanning, signature matching, AI classification, and logging. Easily extensible for future features (e.g., advanced AI, cloud signature updates).

NFR5. Security and File Integrity
The scanner must read files in read-only mode during scanning to avoid accidental modification. Quarantine and deletion actions must be confirmed by the user before execution.

NFR6. Platform Compatibility
The system is intended to run exclusively on Windows OS.

NFR7. AI Enhancement Capability
The system should allow for future integration of advanced AI models to improve detection and reduce false positives.
