User Uploads File(.exe | .txt | .pdf)

|

We Generate Hash of the file

|

Check Hash in Malware Dataset

|

Match? — Yes - Malicious

| No

Extract Features from File [File size / type / # of strings / suspicious keywords]

|

Run Anomaly Detection Model

|

Prediction: Safe or Suspicious

|

Log on Blockchain

|

Show Result to User [Safe | Malicious | Suspicious (manual check)]

What makes our project different (Maybe)

1 Feature Extraction

Pull out details from the file (size, file type, keywords). Understand the content

2 Static Analysis (Basic)

Look for suspicious patterns. Flags potentially risky code/files.

3 Anomaly Detection (ML)

Use Machine Learning to decide malware

4 Blockchain Logging

Log every scanned file's result. no change in the records.

5 Risk Categorization

More user-friendly (Safe, Malicious, Suspicious (needs review))