AI SafeNet – Intelligent Security Threat Analysis Platform

Introduction

With the rapid growth of digital communication, individuals and small businesses face increasing exposure to cybersecurity risks such as phishing emails, malicious URLs, and suspicious files. Most existing cybersecurity solutions are either too technical or too expensive for non-experts.

AI SafeNet aims to bridge this gap by providing a lightweight, intelligent, and user-friendly platform that analyzes potential security threats using artificial intelligence and automated threat-detection tools.

Problem statement

Cyber threats are becoming more sophisticated, making it difficult for non-technical users to identify attacks such as:

- Phishing emails designed to steal credentials.
- Malicious links that lead to malware or fake login pages
- Suspicious file hashes used as malware signatures
- Abnormal user behavior indicating compromise

Most available tools require technical expertise or expensive enterprise subscriptions. There is a need for an accessible platform that provides quick, reliable, and AI-based threat analysis.

Project objectives

AI safeNet aims to:

- Provide an easy-to-use web interface for scanning text, links, and files.
- Use AI/NLP techniques to detect phishing patterns in messages and emails.
- Analyze URLs to detect malicious patterns or risky characteristics.
- Verify file hashes against known malware databases (e.g., VirusTotal API).
- Offer clear, user-friendly risk assessments such as:
    - Safe.
    - Suspicious.

- Very dangerous

- Visualize results in a dashboard using charts and risk indicators.
- Build a scalable backend architecture using:
  - Laravel (main application).
  - Python Flask (microservice for ML analysis).

Scope of work

1.1 Features.

- **Phishing Email/Text Analysis (NLP Model).**
  - Detect keywords and patterns commonly used in phishing: "urgent", "reset password", "verify account".
  - Identify psychological manipulation patterns.
  - Detect unusual or suspicious sentence structures.
  - Output: Risk score + explanation.
- **URL safety analysis.**
  - Check SSL validity (HTTP vs HTTPS).
  - Detect shortened URLs.
  - Analyze domain reputation (via API or built-in rules).
  - Detect common phishing URL patterns.
  - Output: Safe / Suspicious / Malicious.
- **File Hash Verification**
  - Allow file upload
  - Calculate file hash (SHA256/MD5)
  - Integrate VirusTotal or similar API
  - Output: Known malware / Unknown / Clean
- **User Behavior Monitoring (Phase 2)**

  Simple detection of unusual behavior patterns (optional):
  - Failed logins
  - Suspicious access time

- Unusual device usage

1.2 Dashboard

- Clear visualization of results
- Risk levels displayed with colored indicators
- History of scans
- Exportable reports

System architecture

Backend:

- Laravel
  - Handles user interface, authentication, result storage.
- Flask (Python)
  - Runs the AI/ML model and URL analysis engine.
- API integration
  - VirusTotal or open-source malware signature databases.

Frontend:

- Responsive UI built with Blade templates or Vue.js
- Clean design focusing on simplicity and clarity

Machine learning:

- Model built using scikit-learn, pandas, and NLP tokenization (NLTK / spaCy).
- Lightweight classifiers:
  - Logistic Regression
  - Naive Bayes
  - SVM (optional)

Methodology

Data collection:

- Phishing email datasets

- Malicious URL datasets
- Public malware hash lists

Model training:

- Text preprocessing (tokenization, stemming)
- Feature extraction (TF-IDF)
- Model evaluation and improvement

Integration:

- Flask API for real-time inference
- Laravel routes for front-end submission

Testing:

- Unit tests for ML API
- Security testing for dashboard
- Usability testing with real users

Deliverables

- **Fully functional web platform**
- **AI phishing detection model**
- **URL risk assessment module**
- **File hash verification tool**
- **Dashboard with threat insights**
- **Documentation:**
  - System design
  - API documentation
  - User manual
  - Installation guide

Benefits

- Makes cybersecurity accessible to non-technical users
- Reduces risk of phishing and malware infection

- Saves time for individuals and small businesses
- Introduces a practical use of AI in security analysis
- Can be expanded into a full enterprise solution in the future

Conclusion

AI SafeNet provides an innovative and practical solution to everyday cybersecurity challenges. By combining artificial intelligence, automation, and a simple user interface, the platform empowers users to quickly and confidently evaluate potential threats.

The project demonstrates strong technical depth, real-world usefulness, and scalability for future enhancements.