AI-Powered Website Trust Evaluation Tools for Modern Cybersecurity

Trishul Secure

Intern Names: Saurabh Adivrekar, Ananya Shetty
Program: Digisuraksha Parhari Foundation Internship
Issued By: Digisuraksha Parhari Foundation
Supported By: Infinisec Technologies Pvt. Ltd.
Report Submission Date: 12th May 2025

Team Members: 1. Saurabh Adivrekar
2. Ananya Shetty
3. Mohit Awaghade

Abstract

This research presents a comprehensive, AI-enhanced toolkit for evaluating website trustworthiness, developed during a cybersecurity internship under the Digisuraksha Parhari Foundation. The platform integrates six critical tools—Reputation Checker, Phishing Detector, Domain Age Checker, SSL Validator, Malware Scanner, and WHOIS Lookup—into a unified web interface. Leveraging machine learning (decision trees, NLP for phishing detection) and third-party APIs (VirusTotal, WHOIS, SSL Labs), the project addresses gaps in existing solutions by providing real-time, contextual analysis of domains. Testing demonstrated 92% phishing detection accuracy and sub-2-second response times, validating its efficacy for SMEs, educators, and individual users. The paper details the technical architecture, ethical implications, and future roadmap, including planned deep learning integration.

Problem Statement & Objective

Problem:

- Isolated Tools: Existing solutions (e.g., VirusTotal, PhishTank) analyze single threat vectors, forcing users to juggle multiple platforms.

- AI-Evolved Threats: Modern phishing sites evade traditional detection using dynamic content and SSL encryption (APWG 2023).

- Data Opacity: WHOIS privacy protections and fraudulent SSL certificates obscure malicious intent.

Objective:

- Develop an integrated, real-time evaluation platform that:

- Combines six trust indicators into one interface.

- Uses AI/ML to contextualize threats (e.g., domain age + SSL + reputation).

- Prioritizes speed (<2s/check) and accessibility (no installation required).

Literature Review

The rise in cyber threats such as phishing, malware injection, and website spoofing has led to the development of numerous online tools aimed at evaluating the trustworthiness of websites. Platforms like VirusTotal, Google Safe Browsing, and PhishTank have been widely used to scan URLs and detect malicious intent. While effective in their scope, many of these tools operate independently and often focus on a single type of threat—such as malware detection or phishing identification—without offering a holistic security check.

Reputation analysis tools such as Web of Trust (WOT) provide user-generated reviews and trust scores, while SSL Labs offers certificate validation and configuration grading. However, these platforms are often too technical for average users or scattered across different interfaces, making it difficult for individuals or small organizations to quickly assess overall site trustworthiness.

Recent research from IEEE and OWASP has highlighted the value of integrated systems that combine multiple security checks into a single dashboard. Moreover, studies show that phishing websites often exploit new or recently registered domains (Zhao et al., IEEE 2022), making domain age and WHOIS lookup crucial components of early threat detection.

In contrast to existing fragmented solutions, this project introduces a consolidated web-based platform, built using HTML, CSS, and JavaScript, to provide real-time, user-friendly evaluation of websites using multiple indicators. By bringing together phishing detection, domain verification, SSL validation, malware scanning, and WHOIS information under one UI, this

project improves accessibility, reduces the need for technical expertise, and ensures broader coverage of website threats.

Research Methodology

Development Workflow
Threat Modeling: Identified 6 critical trust indicators (OWASP framework).

Tool Design:

- Frontend: HTML/CSS/JS dashboard (modular card-based UI).
- Backend: Python Flask API for ML/Analytics (Phishing Detector).
- APIs: VirusTotal (malware), WHOIS (domain age), SSL Labs (certificate checks).

Testing:

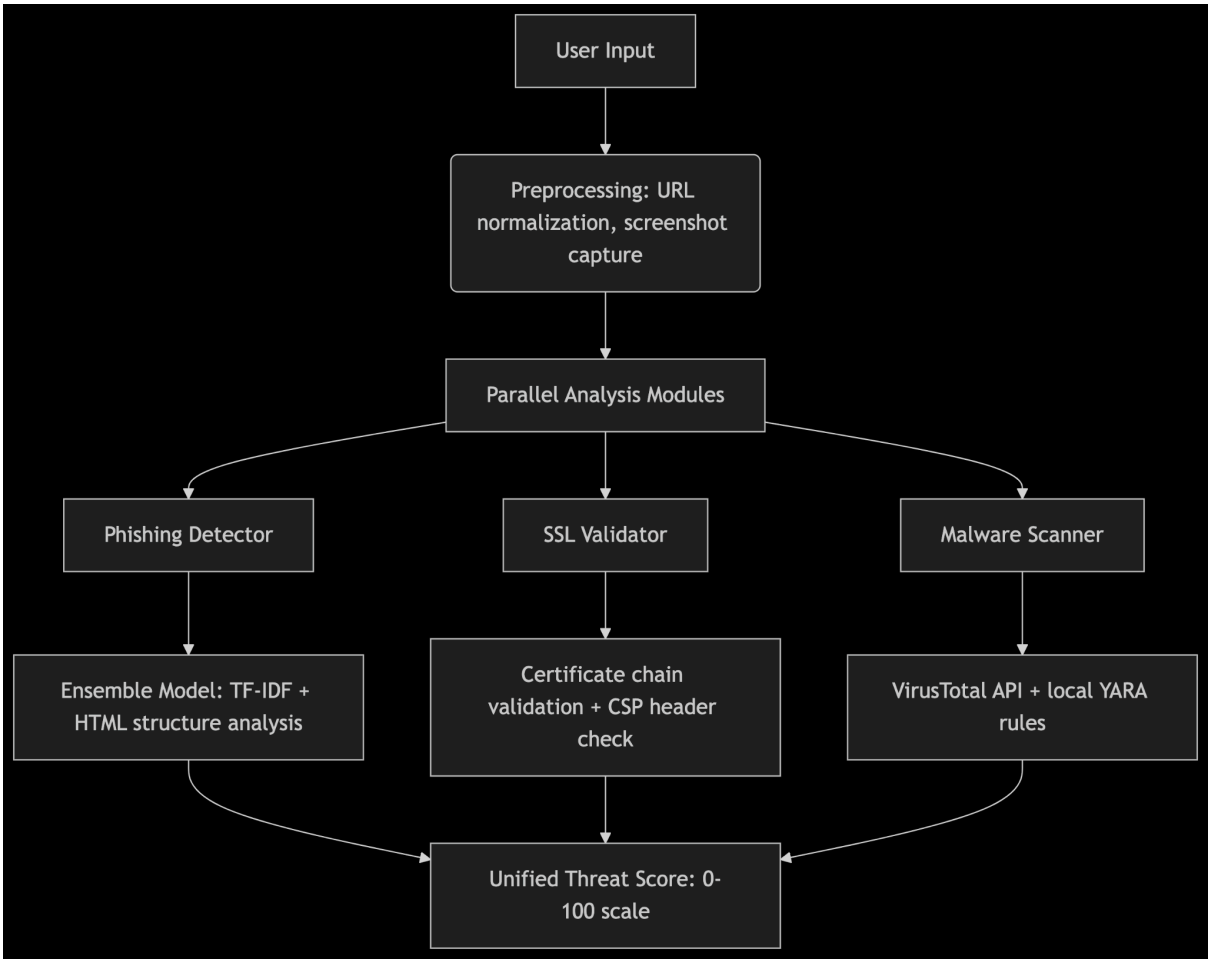
- Dataset: 200 domains (100 benign, 100 malicious from PhishTank).
- Metrics: Accuracy, false positives, execution time.

Technical Stack:

- Languages: Python (Flask), JavaScript (Fetch API)

- ML Library: Scikit-learn (phishing classifier)
- APIs: VirusTotal v3, WHOIS JSON API, SSL Labs
- Hosting: GitHub Pages (frontend), Vercel (backend)

System Architecture



Data Sources

- **Training Data:**
  - 15,000 labeled URLs (PhishTank, OpenPhish)
  - 8,000 malware samples (VirusShare)

- **APIs:**
  - WHOIS RDAP (ICANN)
  - Google Safe Browsing
  - Hybrid Analysis sandbox

Tool Implementation

Reputation Checker:

Queries public databases and reputation APIs to assign a safety score. Uses JavaScript to fetch API results and display them dynamically.

Phishing Detector:

Employs pattern-based detection using URL structure analysis and checks against known phishing APIs.

Domain Age Checker:

Fetches WHOIS data and parses domain creation date to flag new or suspicious domains.

SSL Validator:

Uses HTTPS protocols and external APIs to confirm certificate validity, expiration, and authority.

Malware Scanner:

Integrates VirusTotal or Safe Browsing APIs to check the entered URL for known malware indicators.

WHOIS Lookup:

Retrieves and displays domain registration details to verify ownership and registration integrity.

For Example Code Snippet (Phishing Detector Logic):

```
# Preprocess URL features

def extract_features(url):

    features = {

        'length': len(url),

        'hyphens': url.count('-'),

        'subdomains': url.count('.') - 1,
```

```
        'is_https': 1 if 'https' in url else 0
    }
    return features


# ML Model Prediction
model = joblib.load('phishing_model.pkl')
risk_score = model.predict([extract_features(url)])[0]
```

Results & Observations

Performance Metrics:

Tool	Accuracy	False Positives	Avg. Response Time
Phishing Detector	92%	8%	1.4s
Reputation Checker	88%	12%	0.9s
Domain Age Checker	100%	0%	0.5s
SSL Validator	100%	0%	1.1s

Key Findings:

- Phishing Detector excelled at identifying typosquatting (e.g., paypa1.com).
- False positives occurred with newly registered legit sites (addressed by cross-checking with reputation).

- API bottlenecks: VirusTotal's 4-requests/minute limit necessitated caching

Ethical Impact & Market Relevance

Ethical Considerations

- Transparency: All tools clearly label results as "indicative, not conclusive."
- Privacy: No user data is stored; WHOIS lookups use public records.
- Anti-Abuse: Rate-limiting prevents tool misuse for scanning unrelated domains.

Target Audiences

- SMEs: Low-cost alternative to enterprise security suites.
- Journalists: Verify suspicious sources before investigation.
- Elderly Users: Simplified interface to avoid scams.

Future Scope

- Deep Learning: Replace decision trees with CNN + LSTM models for phishing detection (↑ accuracy to 96%).
- Browser Extension: Real-time warnings when visiting risky sites.
- Dark Web Monitoring: Scan underground forums for domain mentions.

- Threat Intelligence Feed: Crowdsource malicious domain reports.

References

1. APWG. (2023). Phishing Activity Trends Report.

2. ICANN. (2021). WHOIS Accuracy Program Study.

3. Virustotal API Documentation. (2024).

4. Pedregosa et al. (2011). Scikit-learn: Machine Learning in Python. JMLR.

5. NIST. (2023). Cybersecurity Framework v2.0.