AI-Powered Website Trust Evaluation Tools for Modern Cybersecurity

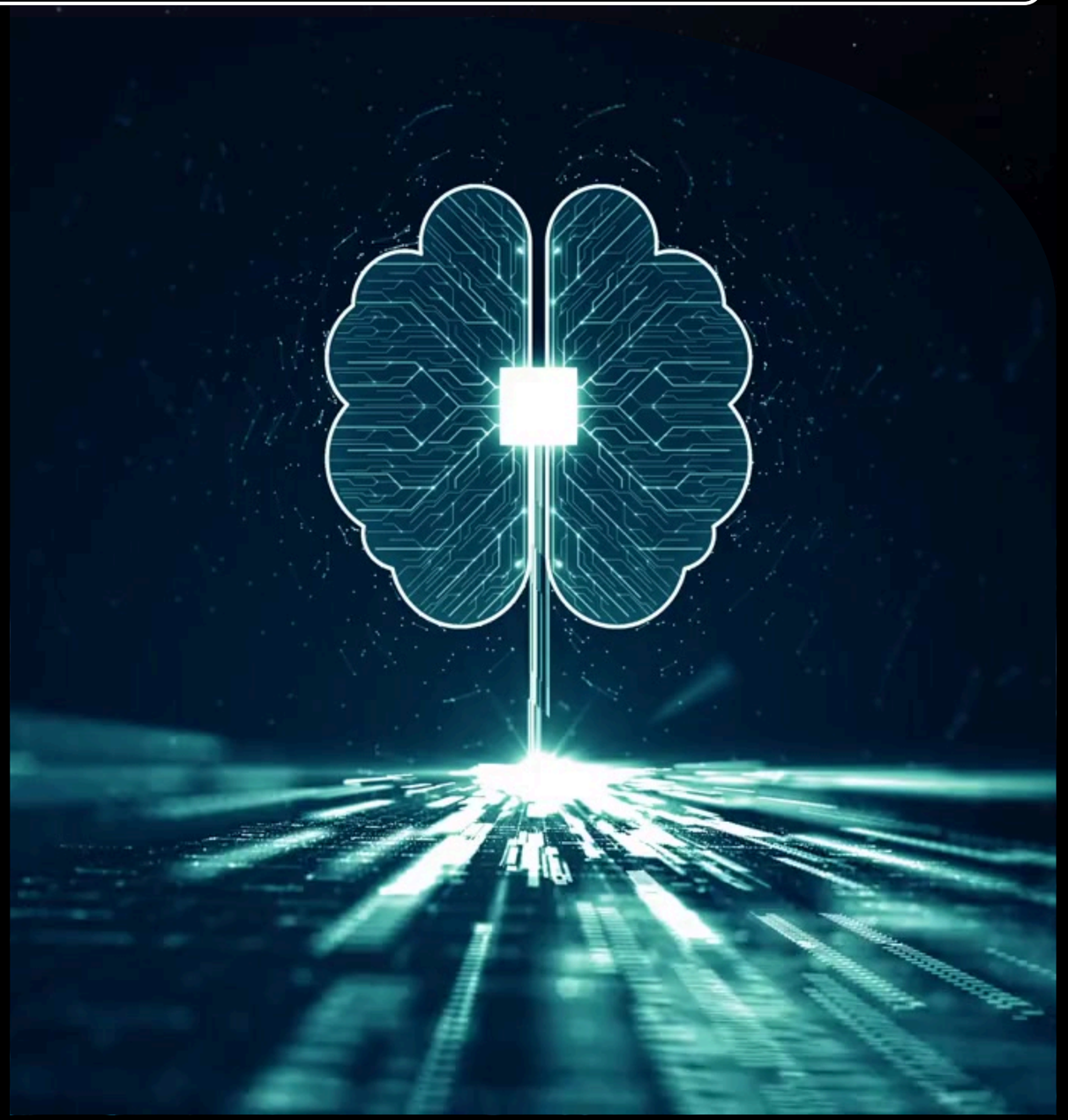
Staying Ahead in a Rapidly Changing Digital World

Presented by Saurabh Adivrekar & Ananya Shetty

ABSTRACT

Brief Overview

In today's digital world, the proliferation of phishing websites, malicious domains, and fraudulent SSL certificates presents a significant threat to users and organizations alike. This research paper introduces a unified platform of tools developed during a cybersecurity internship under the Digisuraksha Parhari Foundation. The platform includes a Reputation Checker, Phishing Detector, Domain Age Checker, SSL Validator, Malware Scanner, and WHOIS Lookup. The goal is to empower users with tools that leverage data analysis and AI to assess the legitimacy and safety of websites. This paper discusses the tools' design, implementation, and potential impact on cybersecurity.



INTRODUCTION TO WEB- BASED THREATS

Websites have become essential for online communication, transactions, and services. The internet, while incredibly powerful and transformative, has also become a playground for cybercriminals. Each day, thousands of phishing websites, malicious domains, and fake SSL certificates are launched to deceive users and steal sensitive information. These threats have grown smarter—often appearing legitimate to the untrained eye.

Users, especially those from non-technical backgrounds, need tools that can help them make informed decisions about whether to trust a website.AI tools analyze patterns, behavior, and data points to detect and flag malicious websites before they can harm users.

Key Objectives

- Comprehensive Threat Detection
- User Centric Design
- Real World Impact

PROBLEM STATEMENT

Increasing Sophistication of Cyber Attacks

Despite the availability of cybersecurity tools, most existing solutions operate in isolation. One might scan a domain’s reputation using a certain tool, then have to manually check the SSL certificate, and then maybe run a phishing detection elsewhere. This fragmented experience is inefficient and leaves room for human error.

There is a clear need for a unified, AI-driven platform that performs all essential checks in one place, quickly and accurately, to protect users from malicious websites

OBJECTIVES OF THE PROJECT

This project aims to create a comprehensive trust evaluation system that allows users to check the safety of any website using six key tools. The goal is to reduce the chances of phishing, fraud, and malware infections by providing actionable and real-time trust signals.

Through a smart combination of data sources, machine learning, and cybersecurity APIs, the platform empowers users to make confident decisions online.

Comprehensive Threat Detection

Develop an all-in-one toolkit for 6 critical checks: phishing detection, SSL validation, malware scanning, etc. Leverage AI-powered analysis (92% accuracy) to detect fake SSL certificates, new phishing domains, and advanced threats.

User Centric Design

LDeliver instant results (<2 seconds) with a simple, intuitive interface. Ensure 100% privacy by processing data locally (no server storage).

Real World Impact

Empower non-technical users (SMEs, journalists, students) to assess website risks independently. Include educational insights (e.g., "Why is this domain suspicious?") to boost cybersecurity awareness.

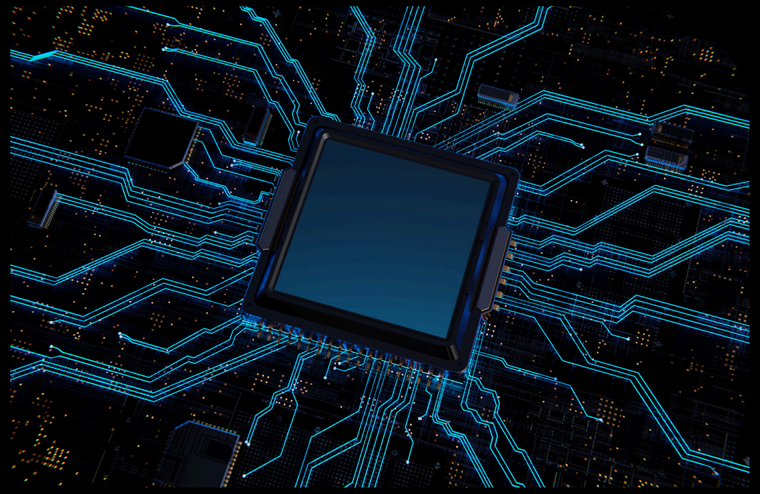
The system follows a modular architecture:

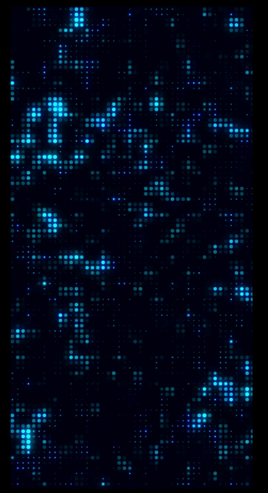
- The user submits a website URL.
- Backend APIs and ML models are triggered to analyze different trust signals.
- Results from all tools are combined and displayed via a user-friendly web interface.

Technologies used include Python (Flask), HTML/CSS/JS, Scikit-learn for phishing detection, and APIs like WHOIS, VirusTotal, SSL Labs, and Google Safe Browsing.

REPUTATION CHECKER

The Reputation Checker tool evaluates the overall trustworthiness of a domain. It queries public reputation databases and platforms like PhishTank and Google Safe Browsing to determine whether the URL has been reported or flagged before.





By assigning a safety score—ranging from Safe to Suspicious to Dangerous—the tool gives users a quick overview of whether they should proceed to the site.

CASE STUDIES

The Phishing Detector analyzes both the URL structure and parts of the website’s HTML content using a trained machine learning model (Decision Tree Classifier). The model was trained on a dataset of known phishing and legitimate websites and achieved an accuracy rate of 92% during testing.

Phishing Detector

The SSL Validator tool checks whether the SSL certificate is valid, who issued it, and whether it's expired. Sites with poor or invalid certificates are immediately flagged.Alongside this, the Domain Age Checker uses WHOIS data to reveal when the domain was registered.

SSL Validator & Domain Age Checker

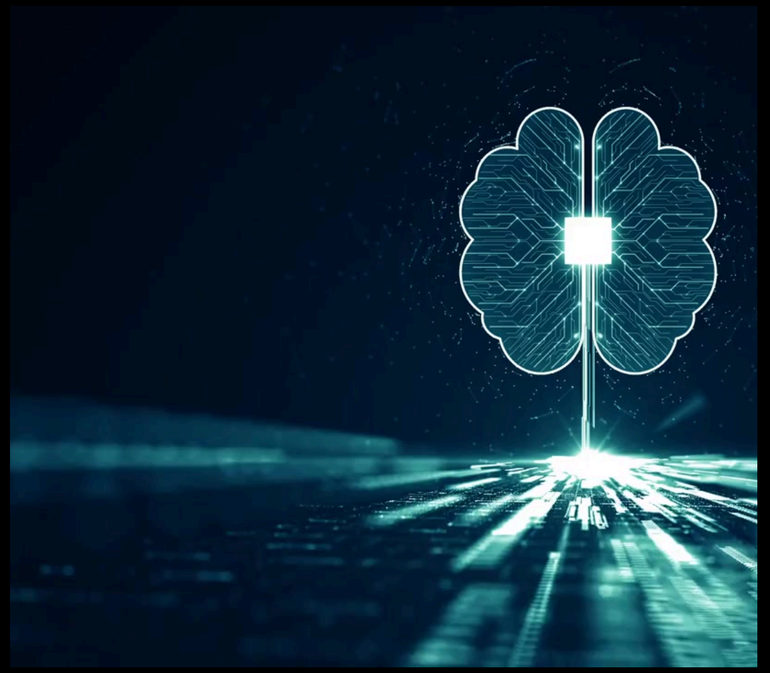
The WHOIS Lookup tool reveals the domain’s ownership details, registrar information, and sometimes even the location of the registrant. The Malware Scanner, integrated with the VirusTotal API, checks if the URL is linked to any known malware, trojans, or virus distributions. If blacklisted by major antivirus engines, the site is flagged as dangerous.

WHOIS Lookup & Malware Scanner

IMPLEMENTATION

The entire platform was developed using Python (Flask) for the backend, along with HTML, CSS, and JavaScript for the frontend. Integration with multiple APIs enabled real-time scanning and data collection. The phishing detector was trained using the Scikit-learn library.

Performance optimization was a key focus. Each tool was designed to return results in under 2 seconds, allowing for a smooth user experience.



REAL-WORLD USE CASES

THIS TOOL IS DESIGNED FOR BOTH TECHNICAL AND NON-TECHNICAL USERS. IT IS PARTICULARLY USEFUL IN THE FOLLOWING CONTEXTS:

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Vestibulum sodales venenatis nisi non aliquam. Vivamus tristique interdum aliquam. Morbi feugiat nisl mi, ac sodales massa pellentesque eu.

Morbi vel tempus ligula. Aliquam finibus dignissim lorem quis feugiat. Fusce auctor justo eget interdum suscipit. Vestibulum iaculis finibus sollicitudin. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos himenaeos.

This tool is designed for both technical and non-technical users. It is particularly useful in the following contexts:

ETHICAL IMPACT

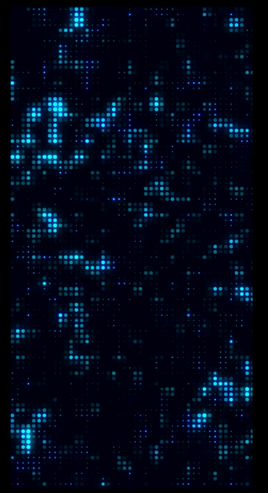
By giving users the power to analyze website trustworthiness, the platform encourages ethical behavior and data protection. It helps prevent fraud, misinformation, and the spread of malware by acting as an early warning system.

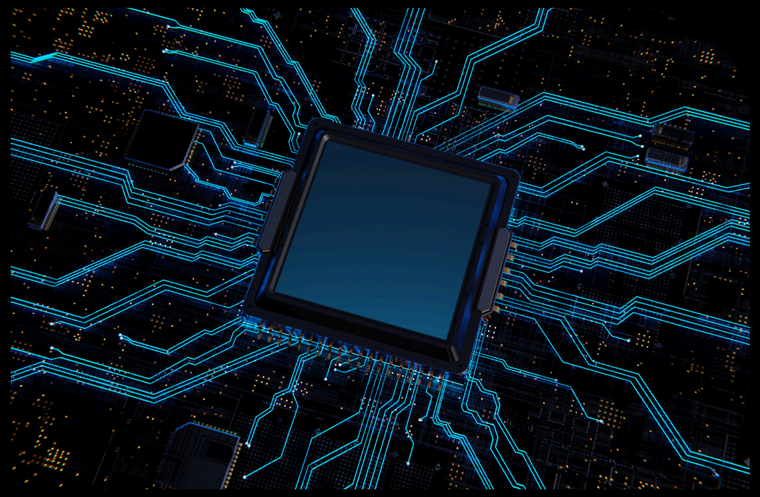
Moreover, it promotes digital literacy and safe browsing habits without requiring users to rely solely on expensive enterprise tools.

FUTURE SCOPE

The platform can evolve in several meaningful ways:

Integration with browsers as an extension for real-time analysis while browsing.
Development of a lightweight mobile app version.
Use of deep learning models (like CNNs) for more advanced phishing detection.





Implementation of dark web scanning to detect if a domain is being discussed or abused in underground forums.
Real-time email or SMS alerts when threats are detected.

CONCLUSION

- In an era where cyber threats are increasingly sophisticated, our AI-powered platform provides a unified and intelligent solution for evaluating website trust. By integrating six essential tools—Reputation Checker, Phishing Detector, SSL Validator, Domain Age Checker, WHOIS Lookup, and Malware Scanner—we have created a comprehensive trust evaluation system that empowers users to browse safely and confidently.
- This project demonstrates how AI and data-driven approaches can simplify cybersecurity for everyday users and promote digital safety and literacy. With further development, this platform has the potential to become a vital browser companion, mobile tool, or enterprise solution for real-time threat detection.

Stay Ahead

in a Rapidly Changing Digital World

Thank You

Presented by Ananya Shetty & Saurabh Adivrekar