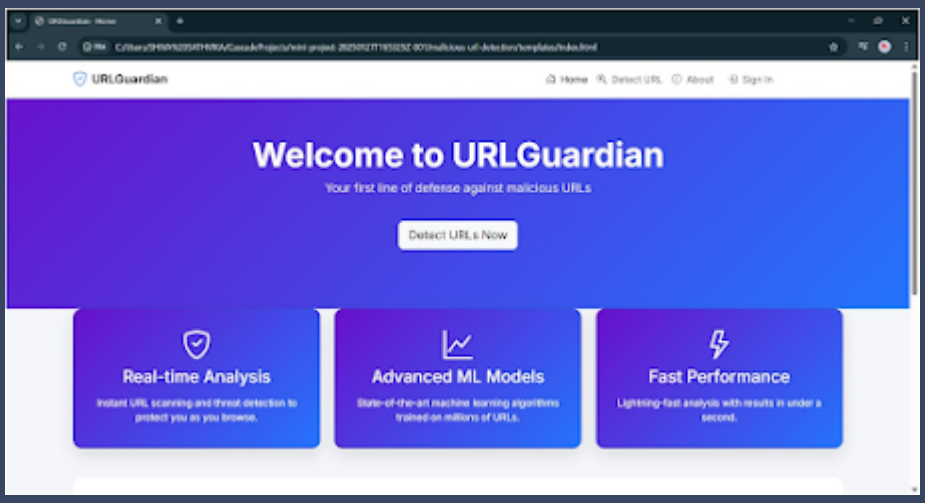
URL Guardian

on March 14, 2025

CYBERSECURITY ENHANCEMENT THROUGH MALICIOUS URL DETECTION WITH ML

The internet is a vital part of our daily lives, but it also comes with dangers. Cybercriminals create fake websites to steal personal information, install malware, and scam users. These harmful websites are often hidden behind deceptive URLs, making them difficult to detect with traditional security methods.

To tackle this problem, our project **"Cybersecurity Enhancement Through Malicious URL Detection with Machine Learning"** introduces an advanced system that automatically identifies and blocks dangerous URLs before they cause harm.



Why is Malicious URL Detection Important?

Every year, cyber threats like **phishing, malware attacks, and online scams** cause billions of dollars in financial loss. Traditional methods such as blacklists and manual checking

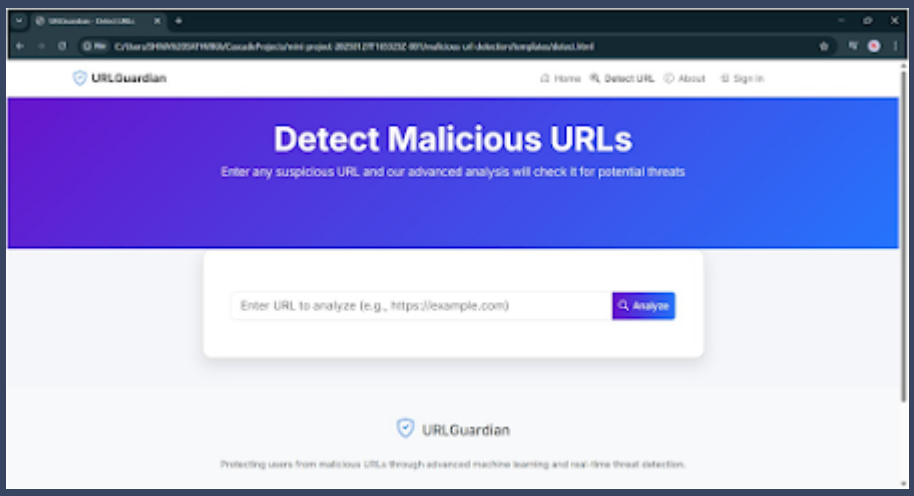
URL Guardian

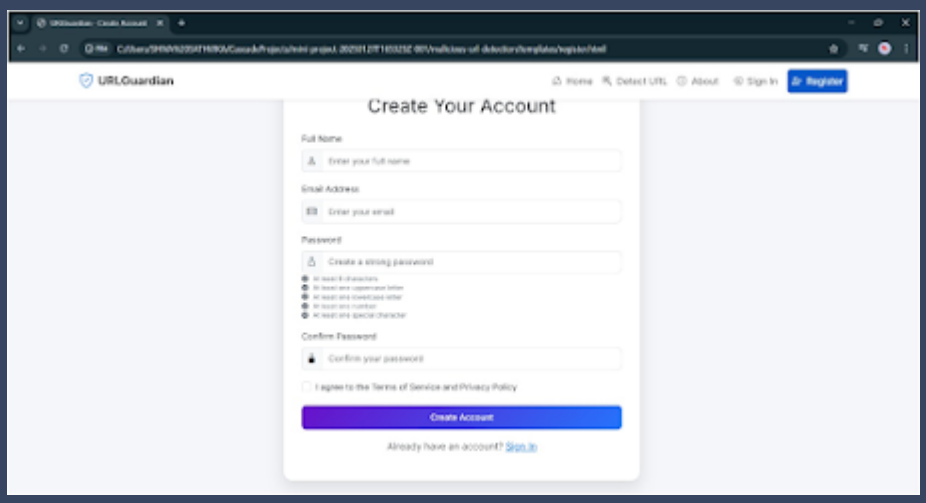
How Our System Works

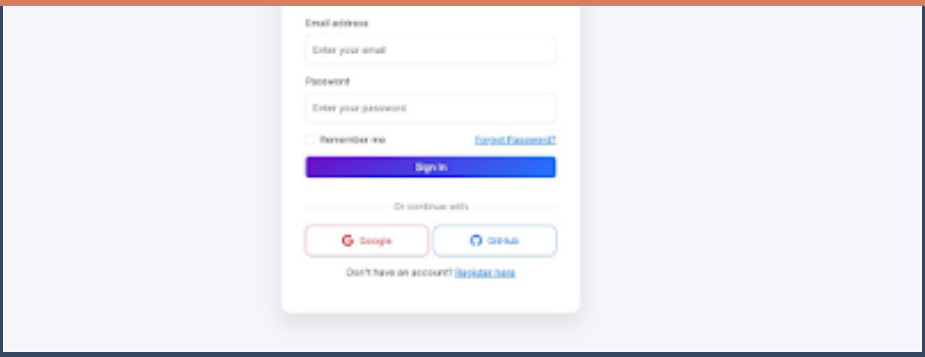
Our system uses **Machine Learning (ML)** to analyze website links (URLs) and classify them as **safe, suspicious, or malicious**. It does this by examining:

- **URL Length** – Malicious URLs are often unusually long.
- **Special Characters** – Suspicious symbols like @, -, and _ may indicate a fake website.
- **Domain Age** – New websites may be risky.
- **Numbers in the URL** – Many scam sites use random numbers in their links.
- **Popularity Ranking** – Trusted websites are generally well-known and frequently visited.

Additionally, we check the website's **SSL certificate validity, redirection patterns, and hosting details** to ensure accuracy.







Poster: https://drive.google.com/file/d/1d_LPzA4hHNVdUjPoX2yBEI8CES11jjjf/view?usp=sharing

Machine Learning in Action

Our system uses advanced **Machine Learning models** like:

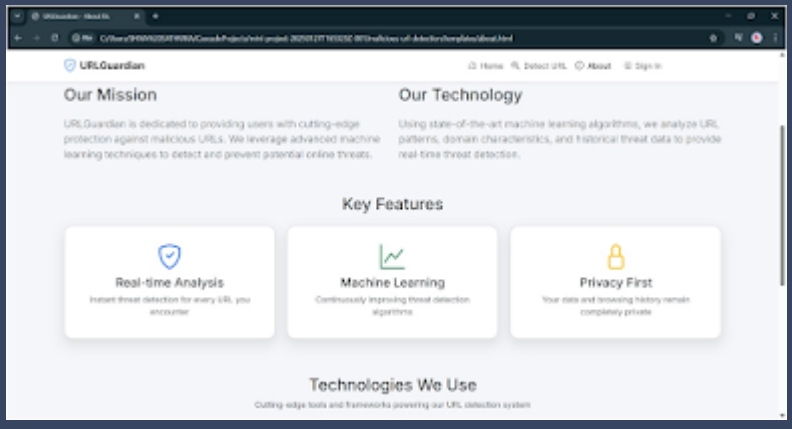
- **Random Forest** – Learns from past data and improves over time.
- **Support Vector Machines (SVM)** – Classifies URLs with high accuracy.

Algorithm Used	Accuracy obtained
Naïve Bayes Classifier	82.6%
Decision Tree	95.4%
Random Forest Classifier	96%
K Nearest Neighbor Algorithm	95.5%

By continuously learning from new threats, these models enhance cybersecurity protection.

Real-Time URL Detection Tool

We have built a **real-time tool** where users can enter a website link and instantly check if it is safe or not. This tool provides a **safety classification and confidence score**, along with insights into why a URL is flagged as harmful.



Future Enhancements

To make the internet even safer, future improvements will include:

- ✅ **Browser extensions** for real-time protection while browsing.
- ✅ **Mobile apps** to check website safety on the go.
- ✅ **AI-powered threat intelligence** that updates automatically with new cyber threats.

Conclusion

By combining **machine learning, security data, and real-time analysis**, our project provides a **powerful solution for detecting and blocking malicious URLs**. This ensures that individuals and businesses can browse the internet safely without falling victim to cyber threats.

The future of cybersecurity depends on **automation, AI, and continuous learning** and with our system, we are taking a step toward a **safer digital world**!

Enter Comment