PHISHING URL DETECTION USING MACHINE LEARNING

TEAM LEADER : DHIVYASHRI S
TEAM MEMBERS: DEVASHRI S
SULAKA B
YUVASREE P

PROBLEM STATEMENT

. Phishing attacks are a growing threat online, targeting people and organizations.

. Attackers trick users into giving personal info like passwords and bank details.

. Current methods use blacklists, which can’t detect new or updated phishing sites.

. Most users don’t have the skills or tools to check if a link is safe.

. There’s no easy-to-use system that checks URLs in real time using smart methods.

. Many existing tools are manual or only for big companies, not regular users.

. So, there’s a strong need for a smart, automatic system that detects phishing websites quickly and easily.

INDIA TODAY

Magazine | Live TV | Search

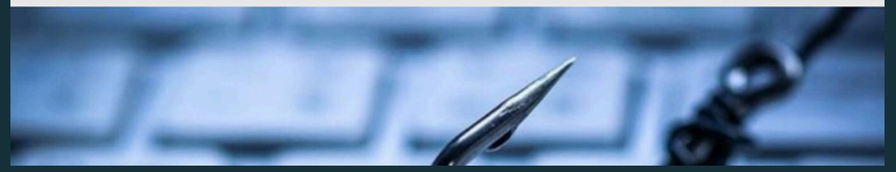
News / Technology / News / India recorded over 79 million phishing ...

India recorded over 79 million phishing attacks in 2023, new study suggests

A significant rise in online scams was observed in India in 2023, with the country recording over 79 million phishing attacks. The Indian government and businesses have responded by implementing cybersecurity measures such as the Digital Personal Data Protection Act and zero-trust strategies to combat these threats.

Listen to Story

Share



Reuters

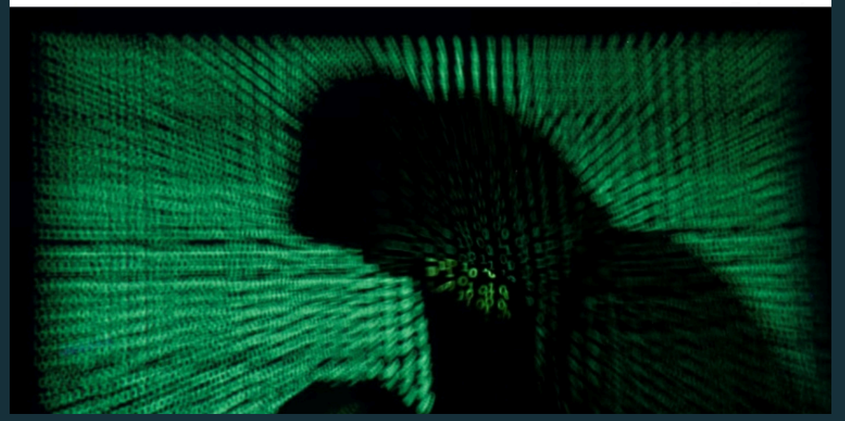
My News

Irish debt office to review security protocols after losing 5 million euros in phishing attack

By **Reuters**

July 15, 2025 3:46 AM GMT+5:30 · Updated July 15, 2025

Aa



ETPrime

INDIA

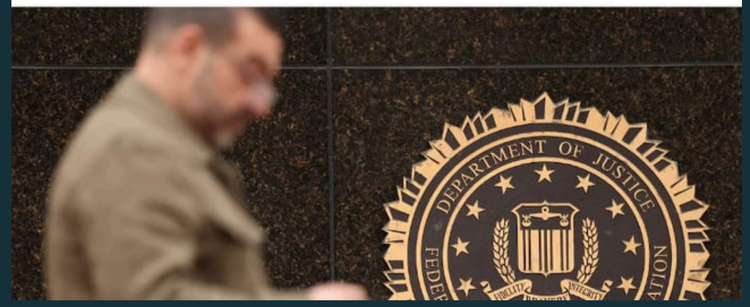
1,172 phishing domains detected in H1: National Technical Research Organisation

Reuters My News

FBI says cybercrime costs rose to at least $16 billion in 2024

By **Reuters**

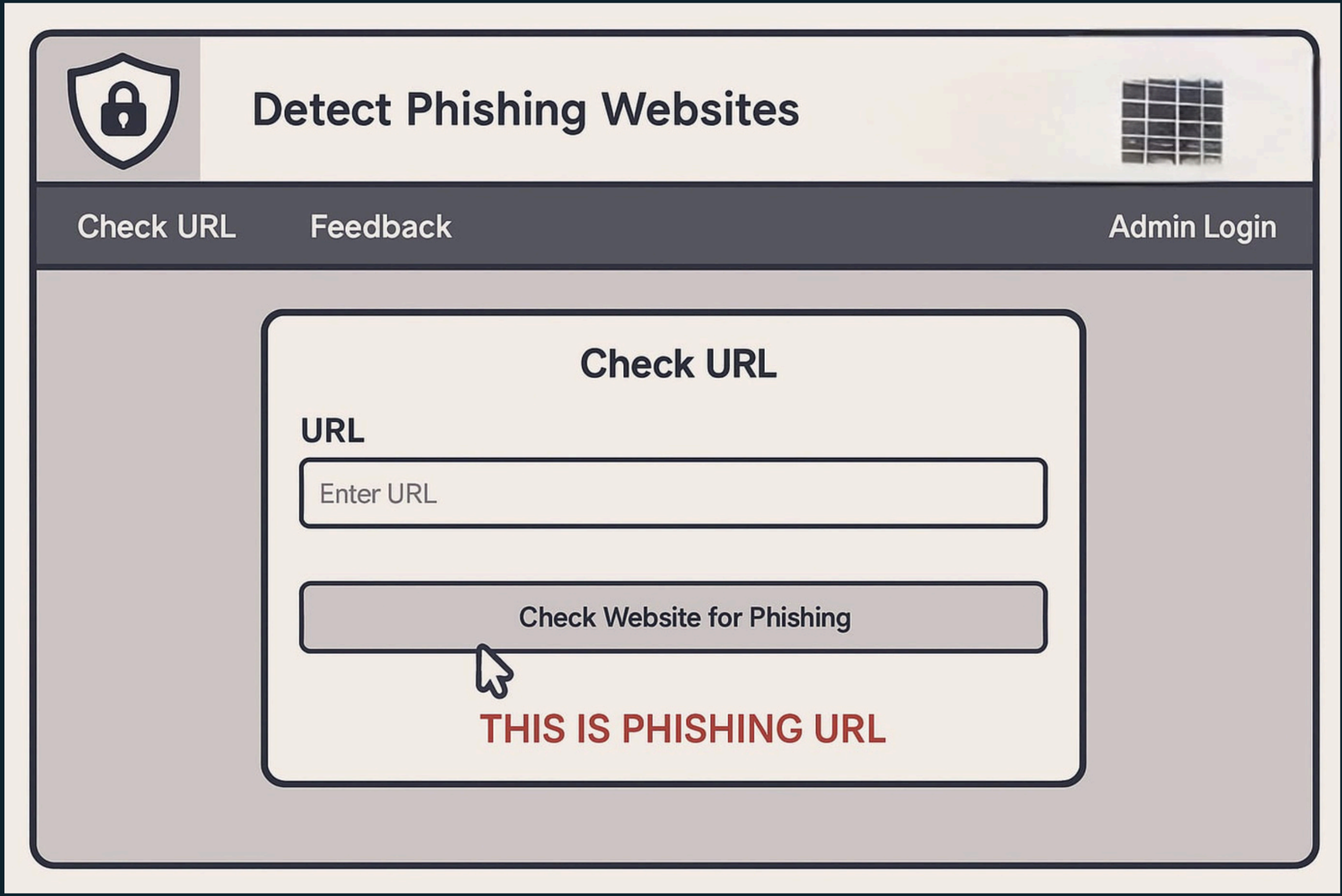
April 23, 2025 5:50 PM GMT+5:30 · Updated April 23, 2025



SOLUTION

The solution uses machine learning and real-time analysis to detect phishing URLs. It includes an admin panel and a user-friendly interface, checks URLs using trained models, verifies SSL (Chrome encryption), and stores results in a database. It’s fast, adaptive, and easy to use.

HOW PHISHING URLs WORK



Detect Phishing Websites

Check URL Feedback Admin Login

Check URL

URL

Enter URL

Check Website for Phishing

THIS IS NOT PHISHING URL

ADMIN PAGE


Detect Phishing Websites
Check URL
Feedback
Admin Login
User Name
Enter Username
Password
Enter Password
URL
Enter URL
Login
Cancel
THIS IS NOT PHISHING URL

TECHNOLOGY USED

Frontend: HTML, CSS, JavaScript

Backend: PHP, Python (via Flask/FastAPI API)

Database: MySQL

ML Libraries: Scikit-learn, XGBoost

Models Used: Random Forest, SVM, XGBoost

Security: Chrome encryption check, HTTPS validation, URL sanitization

Interfaces: Admin Panel + User URL Checker

KEY FEATURES

🧠 ML-Based Detection – Classifies URLs using Random Forest, SVM, XGBoost.

⚡ Real-Time Analysis – Instant phishing check for user-submitted URLs.

🔐 Chrome Encryption Check – Verifies HTTPS and SSL security.

🗂️ Admin & User Interface – Separate panels for managing and checking URLs.

📊 Smart Feature Extraction – Analyzes URL length, domain age, keywords, etc.

📂 Database Support – Stores known phishing/legit URLs for quick lookup.

🔁 Adaptive & Self-Learning – Combines automation with admin input.

📱 User-Friendly Design – Simple, accessible UI for all users.

INNOVATIVE FEATURES

Real-time phishing URL detection

AI/ML-based classification (Random Forest, SVM, XGBoost)

Chrome SSL encryption check

Self-learning system

Admin & user interface

mart feature extraction (HTTPS, domain age, subdomains)

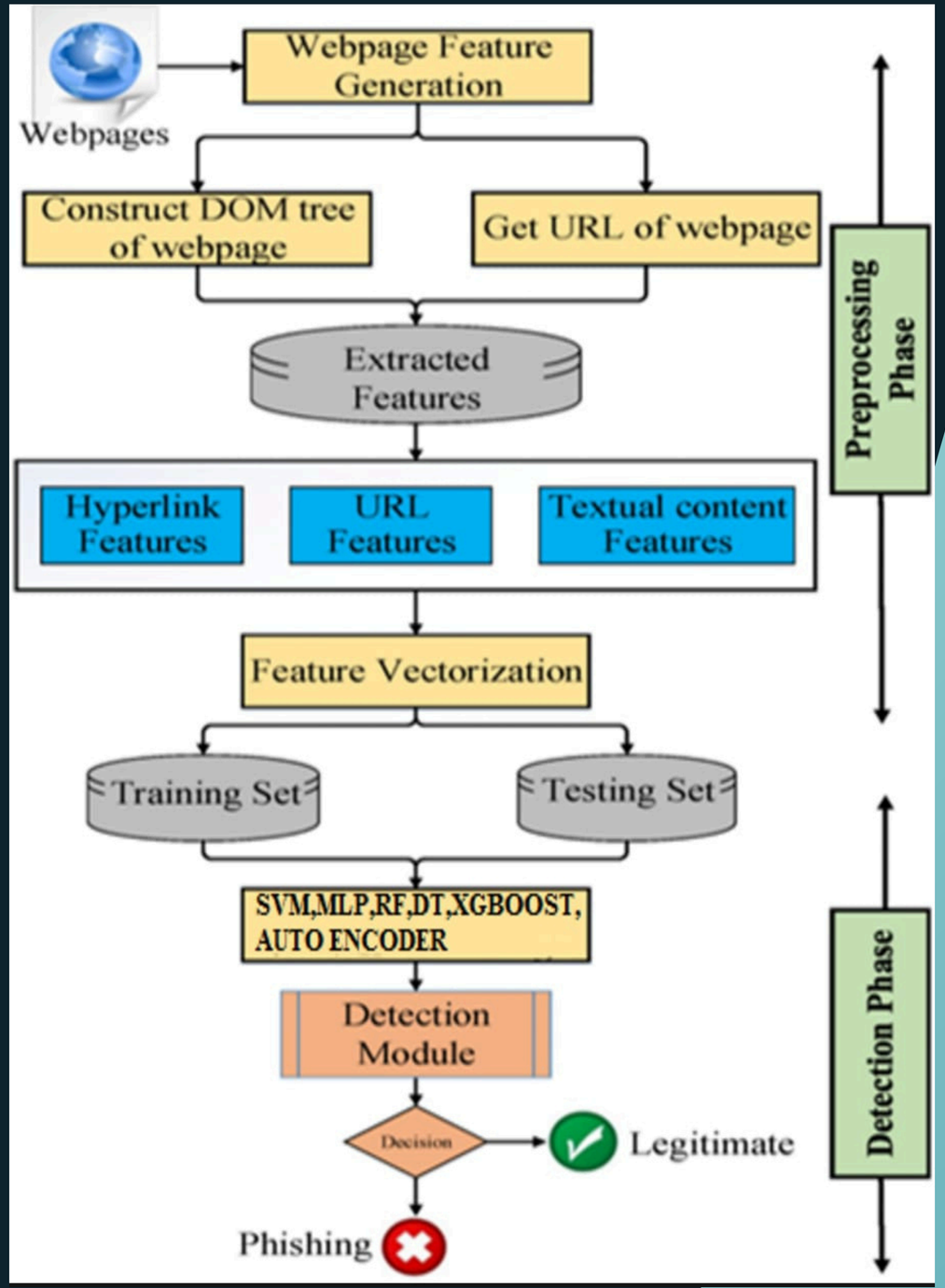
Dual verification: ML + database

Lightweight and scalable design

MOTIVATION

With the rapid growth of internet usage, phishing attacks have become one of the most common and dangerous cyber threats. Existing detection methods like blacklists fail to catch newly generated malicious URLs, leaving users vulnerable. This inspired us to build an intelligent, real-time phishing URL detection system using machine learning, aiming to protect users from fraud, data theft, and cybercrimes through smarter, faster, and more reliable detection mechanisms.

SYSTEM ARCHITECTURE



FUTURE SCOPE

The system can evolve into a browser extension and mobile app with deep learning for improved accuracy, real-time global threat updates, and enterprise features like bulk scanning, APIs, and analytics.

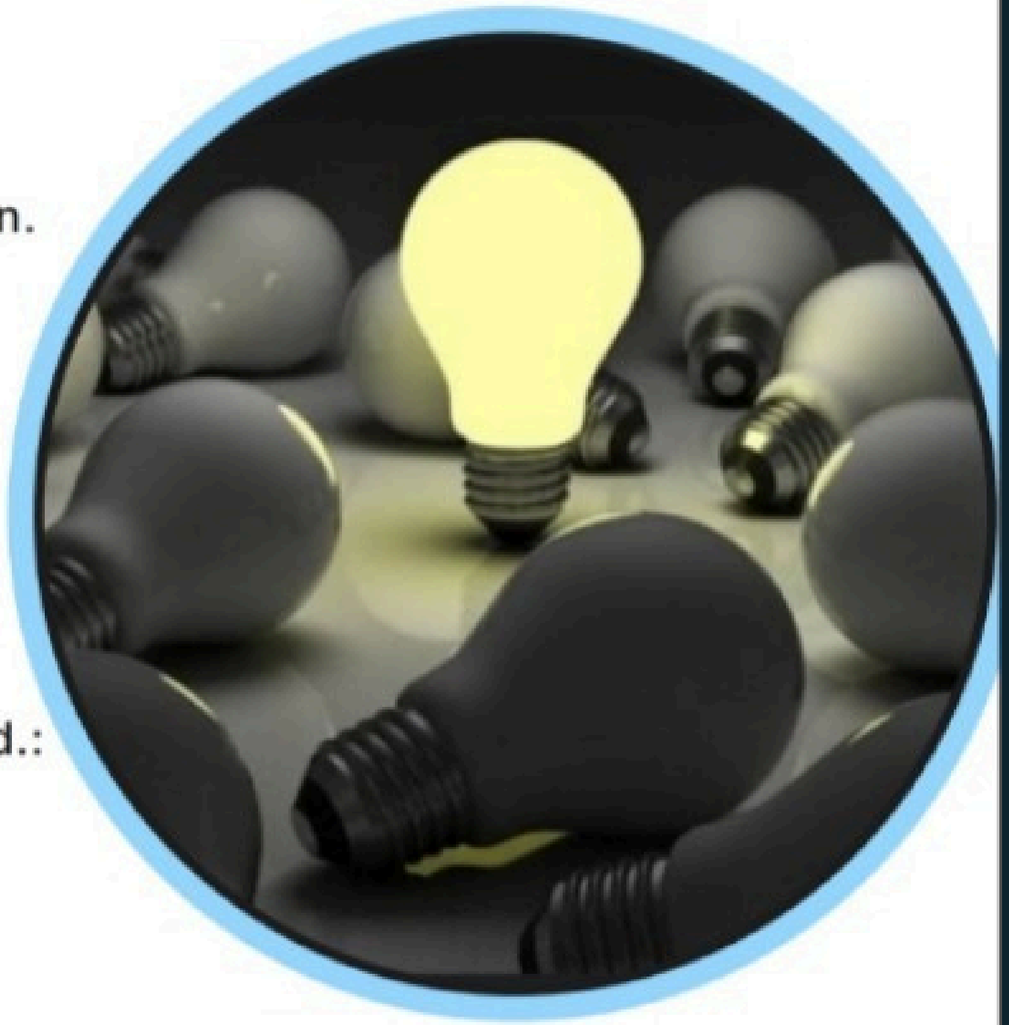
What Makes My Project Unique

Made fully from scratch using PHP, SQL, and Python.

Separate pages for users and admin.

Gives real-time results using machine learning.

Simple to use, good for students and easy to extend.:



Our project

COMPARISON CHART

FEATURES	OTHER PROJECTS	OUR PROJECT
USES PHP FRONTEND	MOSTLY JUST PYTHON ✗	YES ✓
REAL TIME URL INPUT FROM USER	MOSTLY USE CSV FILE ONLY ✗	YES ✓
MACHINE LEARNING MODEL	LOGISTICS REGRESSION OR DECISION TREE ✓	YES ✓
ADMIN PAGE TO MANAGE URL	RARE ✗	YES ✓
SQL DATABASE FOR CROSS CHECK	NOT INCLUDED USUALLY ✗	YES ✓

IMPACT ON SOCIETY 🌎

Just one wrong click can lead to a full data leak.
But many people still don’t take phishing seriously.
🔒 This system helps stop that — by checking links and protecting users.
It can be used in:

- 🏫 Colleges – for awareness
- 🏢 Companies – for employee safety
- 👨‍👩‍👧 Public – for personal protection

It’s more than a project — it’s a digital safety tool for everyone.

TARGET AUDIENCE

Aimed at internet users, students, and organizations to reduce phishing risks, enhance cybersecurity awareness, and promote safe browsing through AI-powered detection.

ROLES OF THE TEAM MATES

1. DEVASHRI.S – Frontend Developer
Responsible for overall coordination, UI/UX design, and implementation of the user-facing URL checker platform using HTML, CSS, and PHP.

2. DHIVYASHRI.S – Team lead & Backend Developer & Database Manager
Handled server-side logic, integration of Python ML models with PHP, and management of the MySQL database for storing URLs and results.

3. YUVASREE.P – Machine Learning Specialist
Developed, trained, and optimized ML models (XGBoost, SVM, Random Forest, etc.) for phishing detection, and conducted performance evaluation.

4. SULAKA.B – Security & Deployment Engineer
Integrated Chrome-based encryption features, handled secure communication between modules, and deployed the system for real-time usage.

CONCLUSION

The Phishing URL Detection System effectively combines machine learning and real-time analysis to identify malicious URLs with high accuracy. With its user-friendly interface and intelligent backend, it enhances online safety for individuals and organizations, offering a scalable and reliable solution to combat phishing threats in today’s digital world.

THANK YOU