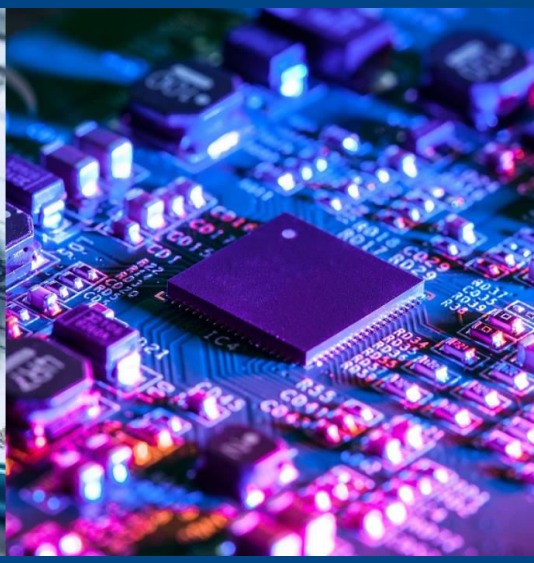
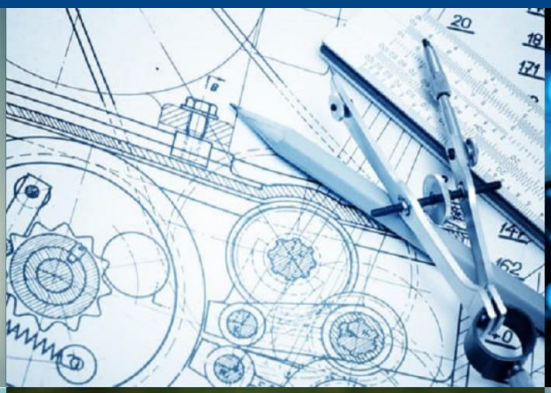
ISSN: 2582-7219

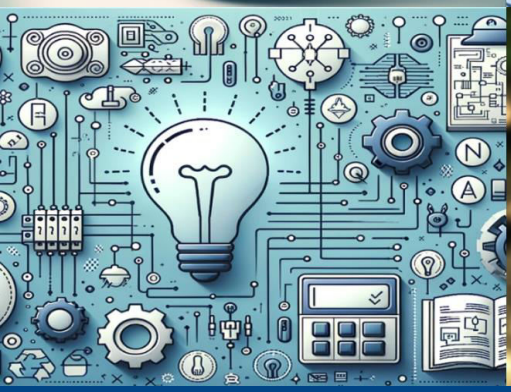




International Journal of Multidisciplinary Research in Science, Engineering and Technology

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.206 **Volume 8, Issue 9, September 2025**

© 2025 IJMRSET | Volume 8, Issue 9, September 2025| DOI:10.15680/IJMRSET.2025.0809034

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Phishing Detection and Cybersecurity: A Hybrid AI Approach for Real-Time Threat Analysis

Dr. S. Chandia[1], Umang Jaiswal N[2], Akshara K[3], Adithya R. K[4], Shifana S[5]

Assistant Professor, Department of Computing (DCS), Coimbatore Institute of Technology, Coimbatore, Tamil Nadu, India[1]

III Year M.Sc. (Decision and Computing Sciences), Department of Computing (DCS), Coimbatore Institute of Technology, Coimbatore, Tamil Nadu, India[2]

II Year M.Sc. (Decision and Computing Sciences), Department of Computing (DCS), Coimbatore Institute of Technology, Coimbatore, Tamil Nadu, India[3–5]

ABSTRACT: The rapid growth of digital transactions has increased phishing threats in which attackers can leverage obfuscated URLs, false domains, and invalid SSL certificates. Existing security measures based on blacklists have not been effective in defending against newly provisioned malicious sites. In this work we develop a real-time phishing detection API using FlaskH, which incorporates a WHOIS check, a SSL validation, a VirusTotal reputation check, and Google Safe Browsing. There is a hybrid machine learning model based on using TF-IDF and Logistic Regression, along with a fine-tuned BERT model for enhanced phishing detection performance. It also uses a docker sandbox to analyze websites and have defined explainable output. The system demonstrated a safe, secure, scalable, and robust solution for addressing emerging phishing attacks.

KEYWORDS: Phishing Detection, Machine Learning, BERT, Real-time Security, Explainable AI

I. INTRODUCTION

The exponential growth of online transactions and digital services has resulted in a massive growth in phishing websites, scam portals, and insecure links that mislead users into sharing their sensitive details like banking passwords, UPI PINs, and OTPs. Phishing websites and portals usually employ methods such as URL obfuscation, spoofed domains, expired SSL certificates, and malicious redirects to evade current security controls. Existing browser-based defenses are mostly reactive based on blacklists that do not pick up newly generated or encoded malicious domains in real time. This makes users, especially less technically skilled users, extremely susceptible to financial scams, identity theft, and data breaches. Thus, there is a dire need for a real-time, multi-layered phishing detection system which can dynamically analyze URLs, check for domain legitimacy, check SSL certificates, incorporate threat intelligence feeds, and display straightforward Safe/Unsafe outputs for better user protection.

II. LITERATURE REVIEW

A critical assessment of the work done so far on phishing website detection has been carried out to relate how the current study builds upon existing research. With the rapid growth of online transactions, phishing attacks have become a major cybersecurity threat. Numerous tools and techniques have been developed, ranging from database-driven URL checkers to advanced artificial intelligence models. While blacklist-based methods and free URL checkers offer accessible solutions, they often fail to detect new and sophisticated phishing attacks. AI-based systems provide higher adaptability, yet they may face challenges in explainability and false positives. Despite significant progress, there is still a large scope for improvement, especially in developing scalable, real-time, and explainable phishing detection systems.

Bolster AI (2025), in its phishing detection tool *CheckPhish*, demonstrated how artificial intelligence significantly improves the accuracy of identifying malicious websites by analyzing URL structures, behaviors, and real-time

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

threat feeds [1]. The study emphasized AI's role in shaping cybersecurity strategies and proactive defense. **Relevance to Current Research:** The present work builds on this by adopting hybrid ML and BERT-based models to enhance detection accuracy while ensuring real-time adaptability.

EasyDMARC (2025) presented a free phishing URL checker, focusing on accessibility and rapid classification of suspicious links [2]. Its strength lies in ease of use and applicability for SMEs. **Relevance to Current Research:** The current study integrates similar lightweight checks (WHOIS, SSL validation) but enhances them with ML and API-driven automation for enterprise-grade scalability.

Skysnag (2025) introduced a phishing check tool that relies on URL inspection and threat intelligence databases [3]. The study highlighted database-driven detection reliability but pointed out slower adaptability to zero-day phishing URLs.
Relevance to Current Research: Our system addresses this limitation by supplementing database lookups with ML-based predictions for unknown domains.

E. Swarchandt (2021) provided a publicly available Kaggle dataset for phishing detection, enabling benchmarking and development of ML algorithms [4]. This dataset has been widely adopted for model training and evaluation.
Relevance to Current Research: The present research also leverages public datasets for training but extends the approach with real-time verification modules.

Shreya Gopal (2022) developed a GitHub repository showcasing ML classification techniques for phishing detection [5]. The project compared algorithms on real datasets, emphasizing feature engineering and accuracy trade-offs.
Relevance to Current Research: This inspires the integration of TF-IDF and Logistic Regression in our hybrid model, while addressing gaps in scalability and deep learning adoption.

No.	Paper Title	Author(s)	Key Points	Remark
1	CheckPhish – Phishing Detection Tool	Bolster AI, 2025	AI-driven detection using URL and behavioral analysis [1]	Demonstrates effectiveness of AI-based proactive defense
2	Phishing URL Checker	EasyDMARC, 2025	Free, accessible tool for SMEs to detect suspicious links [2]	Useful for small businesses, but lacks scalability
3	Phishing Check Tool	Skysnag, 2025	Database-driven phishing URL verification [3]	Reliable but slower against zero-day threats
4	Phishing Website Detector Dataset	E. Swarchandt, 2021	Public dataset supporting ML-based phishing research [4]	Valuable for benchmarking and model training
5	Phishing Website Detection by ML	Shreya Gopal, 2022	ML-based classification techniques with performance comparisons [5]	Highlights practical gaps in feature selection and scalability

In summary, the reviewed studies show progress in phishing detection ranging from simple URL-based tools to AI-powered systems. While datasets and ML-based methods have improved detection accuracy, challenges remain in scalability, explainability, and adaptability to zero-day attacks. The current research addresses these gaps by combining lightweight verification, hybrid ML-BERT models, and explainable real-time outputs, contributing a proactive and scalable phishing defense framework.

III. OBJECTIVES

- To develop a Flask-based real-time phishing detection API.
- To implement URL decoding and domain legitimacy checks using WHOIS data.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

- To evaluate domain reputation and SSLcertificate validity.
- To integrate Google Safe Browsing and external threat intelligence sources for enhanced verification.
- To provide a multi-layered risk evaluation system that outputs Safe/Unsafe results for user protection.

IV. METHODOLOGY OF PROPOSES SURVEY

URL Collection and Preprocessing

The system starts by gathering URLs via a Flask API endpoint. Encoded or obfuscated URLs are decoded by Base64 methods, and domains are removed for closer examination. ***Data Sources:*** Browser extensions, PhishTank dataset, Kaggle phishing URL dataset, and user-provided inputs.

Domain Legitimacy Verification

Domain legitimacy is checked through WHOIS lookups to confirm registration information, ownership, and age of the domain. Newly registered domains, usually linked to scams, are considered suspicious. ***Data Sources:*** WHOIS registry databases.

Reputation and Security Checks

External threat intelligence is incorporated into the system to analyze domain safety. VirusTotal API is used to perform reputation checks, SSL certificate validation provides encrypted connections, and URLs are cross-checked with Google Safe Browsing API for known hosts of phishing or malware. ***Data Sources***: VirusTotal, Google Safe Browsing, SSL certificate authorities.

Machine Learning Analysis

A hybrid machine learning level increases phishing detection. TF-IDF with Logistic Regression detects suspicious patterns in URLs, while a fine-tuned BERT model detects semantic meaning in phishing-content webpages. The two models are combined using an ensemble method to increase accuracy and minimize false positives[7]. ***Data Sources:*** PhishTank, UCI Machine Learning Repository, Kaggle phishing datasets, and custom-collected URL samples.

Risk Evaluation and User Protection

Results from all modules are combined into a final risk score. Unsafe URLs are blocked with explainable notifications indicating the reason (e.g., invalid SSL, malicious reputation), whereas safe URLs are permitted smoothly. The system also involves user feedback and crowdsourced intelligence to update the threat database continuously. ***Data Sources***: Real-time user reports and community-driven submissions.

V. TOOLS FOR ANALYSIS

Programming and Frameworks

Python is used as the core programming language for development. Flask serves as the backend framework to build the phishing detection API, while Flask-CORS is employed to enable secure communication between the backend and frontend (such as a browser extension)[1].

Libraries for Web and Data Processing

The system utilizes several Python libraries for web interaction and data handling. The Requests library is used to fetch webpage content and perform HTTP requests. BeautifulSoup (bs4) is applied for extracting and parsing webpage text. Whois is used to retrieve domain registration details and age, while Regex (re) helps identify suspicious URL patterns. Additionally, the base64 library decodes encoded or obfuscated URLs.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Security and Threat Intelligence APIs

Security checks are enhanced by integrating external APIs. The VirusTotal API provides domain/IP reputation and malicious activity reports. The Google Safe Browsing API detects phishing, malware, and unsafe websites. SSL certificate verification is also employed to ensure secure HTTPS connections[10].

Machine Learning and Natural Language Processing

For machine learning, Scikit-learn is used to implement TF-IDF vectorization and a Logistic Regression classifier. The Transformers (BERT) library enables deep semantic phishing detection using natural language processing. An ensemble learning approach is adopted to combine TF-IDF and BERT outputs for improved accuracy[5].

Deployment and Execution Tools

The system is deployed and tested using modern tools. Docker provides sandbox execution to safely run and inspect suspicious websites in isolated environments. Postman is used for testing API endpoints and verifying system integration[9].

VI. INFERENCE

A layered security approach is critical to effective phishing detection. While basic protections with WHOIS, SSL checks, and Google Safe Browsing are better than nothing, they are not sufficient against the rapidly evolving phishing methods that are used today. By leveraging threat intelligence APIs (VirusTotal) in conjunction with machine learning (TF-IDF and Logistic Regression) and deep learning (BERT), the system can provide rapid detection with contextual insight, while Docker-based sandboxing allows for safe URL analysis, and Flask serves as the framework for real-time deployment. The use of AI, as well as explainable alerts, along with traditional checks, should provide a robust and scalable solution for protecting users against phishing, fraudulent payment sites, and other cyberattacks.

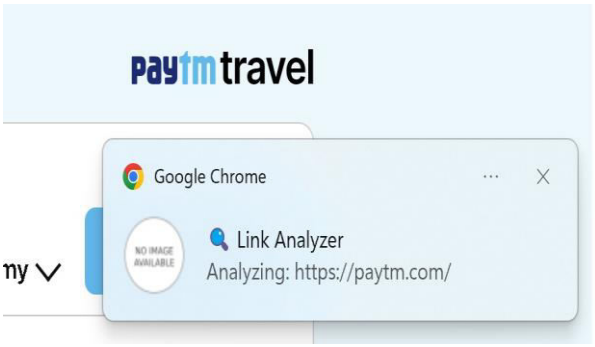


Fig 1.1 Real-Time URL Analysis Using Link Analyzer

Fig 1.1 demonstrates the Link Analyzer tool analyzing the official Paytm website URL. The analyzer verifies the safety of the link, ensuring that it is free from malicious redirects, phishing patterns, or unsafe content. Such validation is essential for popular payment platforms where fraudulent look-alike sites are commonly used in phishing attacks. This process highlights how link analyzers contribute to building user trust by confirming the authenticity of high-traffic financial websites. Ultimately, it ensures that users can access services like Paytm safely and securely.

© 2025 IJMRSET | Volume 8, Issue 9, September 2025| DOI:10.15680/IJMRSET.2025.0809034

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

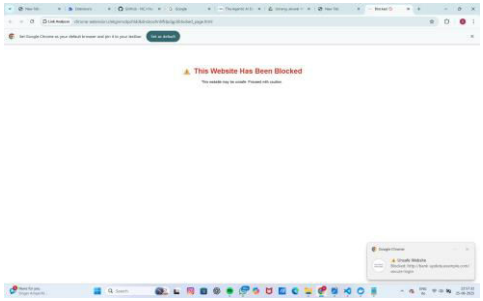


Fig 1.2 Unsafe Website Blocked by Link Analyzer

Fig 1.2 shows the Link Analyzer tool actively blocking access to a potentially unsafe website. The warning message indicates that the detected link may host phishing content or malicious activity, advising the user to proceed with caution. This demonstrates the effectiveness of the tool in preventing users from interacting with fraudulent domains that mimic banking or financial services. By blocking the connection before the website loads, the tool reduces the risk of credential theft and other cyberattacks. Such functionality is crucial in real-time phishing prevention and end-user protection.

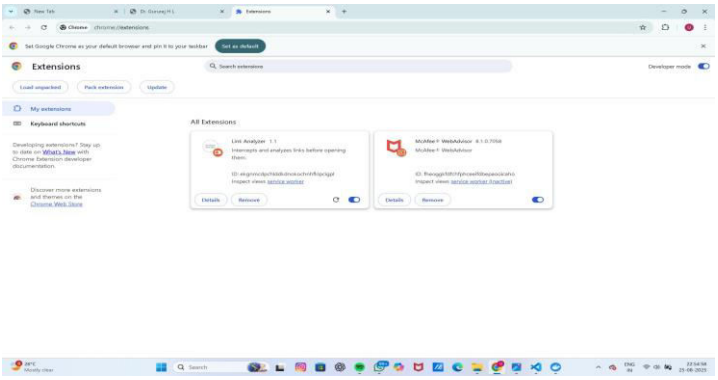


Fig 1.3 Chrome Extensions Page

Fig 1.3 shows the list of extensions installed in the Google Chrome browser. It includes the Link Analyzer (v1.1), which intercepts and analyzes links before opening them, and McAfee WebAdvisor, a widely used security extension. The figure highlights how multiple security extensions can work together to provide layered protection against phishing attacks and unsafe websites. This setup ensures that both real-time link scanning and broader web safety checks are active within the browser environment.

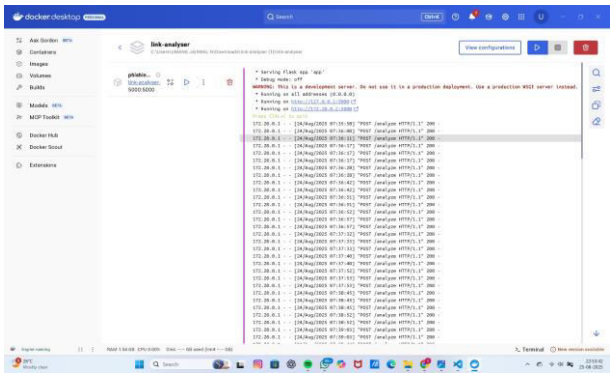


Fig 1.4 Docker desktop container running link-analyzer with flask server logs

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Fig 1.4 shows the execution logs of the link-analyser container running on Docker Desktop. The application is served using a Flask development server and is accessible locally via http://127.0.0.1:5000 and on the network through http://172.20.0.2:5000. The console logs indicate multiple successful POST requests to the /analyze endpoint, each returning a status code 200, which confirms proper functioning of the phishing URL detection module.The warning displayed emphasizes that Flask's development server should not be used in production, highlighting the need for a more secure deployment using a production-ready WSGI server.This step validates the operational aspect of the phishing detection system within a containerized environment.

VII. FINDINGS AND SUGGESTIONS

The present article illustrates that a multi-layered phishing detection system is superior to a single-point security check. The existing methods in this area, like WHOIS searches, SSL certification verification, and Google Safe Browsing rely on basic threat intelligence, but these methods only account for static threat intelligence and will not adequately detect newly generated phishing domains or obfuscated URLs. A multi-layered IPA is designed to address both these problems. By utilizing VirusTotal as a source of threat intelligence, the accuracy of the machine learning methods introduced, like TF-IDF with Logistic Regression and BERT, in conjunction with researchers having domain knowledge of malicious content, improved accuracy, detection, and output. The sandboxing aspect, also based on the use of Docker, further increases the system's efficiency by allowing the execution of suspicious sites in isolation and safe execution, noting if they are indeed malicious. To summarize, that a combination of traditional, rule-based methods, and modern, AI-driven methods creates a more secure, scalable, and active defence against both phishing attacks and fraudulent payment portals is the key takeaway from this research.

VIII. CONCLUSION AND FUTURE WORK

This research demonstrates that a multi-layered phishing detection system that employs rule-based checks, threat intelligence APIs, and AI models brings a high level of protection against today's cyber threats. Using WHOIS, SSL verification, Google Safe Browsing, TF-IDF with Logistic Regression, and BERT achieves better accuracy and explainability than models relying solely on AI, while making it still usable by non-technical users. Additionally, Docker sandboxing provides a secure inspection environment, and Flask APIs make it easy to deploy in real time.

Future work will focus on increasing the diversity of the dataset employed, integrating live-threat intelligence updates, and enhancing the user experience through a browser extension or mobile application for more rapid and proactive phishing detection.

REFERENCES

[1] Bolster AI, "CheckPhish – Phishing detection and prevention tool," Available: https://checkphish.bolster.ai/
[2] Check Point, "Phishing Detection Techniques – Cyber Hub," Available: https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-phishing/phishing-detection-techniques/
[3] EasyDMARC, "Phishing URL Checker – Free tool to detect phishing links," Available: https://easydmarc.com/tools/phishing-url
[4] E. Swarchandt, "Phishing Website Detector Dataset," Kaggle, 2021. Available: https://www.kaggle.com/datasets/eswarchandt/phishing-website-detector
[5] IEEE Xplore, "Phishing Website Detection Techniques," 2025. Available: https://ieeexplore.ieee.org/document/10735206/
[6] NordVPN, "Phishing Link Checker-Detect malicious URLs," Available: https://nordvpn.com/link-checker/?
[7] PhishGuard, "PhishGuard: A Multi-Layered Ensemble Model for Optimal Phishing Website Detection," arXiv preprint, 2024. Available: https://arxiv.org/abs/2409.19825
[8] Shreya Gopal, "Phishing Website Detection by Machine Learning Techniques," GitHub Repository, Available: https://github.com/shreyagopal/Phishing-Website-Detection-by-Machine-Learning-Techniques
[9] Skysnag, "Phishing Check Tool – Identify malicious websites," Available: https://www.skysnag.com/phishing-check/
[10] Sucuri, "SiteCheck – Website Security & Malware Scanner," Available: https://sitecheck.sucuri.net/

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

[11] ThreatCop, "Phishing URL Checker – Free tool to detect phishing websites," Available: https://threatcop.com/phishing-url-checker

[12] EXPLICATE, "Enhancing Phishing Detection through Explainable AI and LLM-Powered Interpretability," arXiv preprint, 2025. Available: https://arxiv.org/abs/2503.20796

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com