International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 03 , March - 2026

Real-Time Phishing Website Detection using a Browser Extension with Random Forest Classifier

Ghoshita Pradeep Nerurkar
Dept. of Electronics and Telecommunication
Engineering Ramrao Adik Institute of Technology
Navi Mumbai, India

Dr. Ashwini Naik
Supervisor
Dept. of Electronics and Telecommunication
Engineering Ramrao Adik Institute of Technology
Navi Mumbai, India

***Abstract*—Phishing is one of the most prevalent cybersecurity threats globally, targeting unsuspecting users by impersonating legitimate websites to steal sensitive data. This paper proposes a real-time phishing website detection system implemented as a browser extension, using a Random Forest classifier. The system extracts address bar, domain-based, and HTML/JavaScript fea- tures to classify websites as phishing or benign. Experimental results on a dataset of 6,000 websites yielded an accuracy of 86.1%, with a precision of 81.65%, recall of 93.05%, and specificity of 79.1%. The model is integrated into a Google Chrome extension, providing seamless and immediate phishing alerts to users during browsing.**

***Index Terms*—Phishing Detection, Machine Learning, Random Forest, Browser Extension, Cybersecurity, URL Analysis, Real- Time Detection.**

I. INTRODUCTION

Phishing attacks have become a major cybersecurity chal- lenge in recent years. According to recent reports by the Anti- Phishing Working Group (APWG), the number of phishing attacks has consistently increased, leading to massive financial losses globally. Attackers often create fake websites mim- icking legitimate organizations to trick users into revealing sensitive information such as passwords, banking credentials, or credit card details.

Traditional phishing detection methods rely on blacklists maintained by security organizations. However, blacklist-based solutions are insufficient due to the rapid evolution of phishing URLs, many of which exist for only a few hours. Therefore, machine learning-based approaches capable of detecting zero- day phishing attacks are essential.

In this paper, we propose a machine learning-based phishing detection system deployed as a Chrome browser extension. The system uses a Random Forest classifier, selected for its high accuracy and low latency, making it suitable for real-time applications.

II. RELATED WORK

Several researchers have explored phishing detection meth- ods using machine learning, browser extensions, and behavior analysis.

A. Machine Learning Based Detection

Adarsh Mandadi et al. [1] developed a phishing detection system using Random Forest and Decision Tree classifiers, achieving approximately 85% accuracy. Their system focused on URL features like length, presence of special symbols, and subdomain analysis.

Areti Nagendra et al. [2] used lightweight URL analysis, extracting 10 features for machine learning classification. Their model outperformed traditional systems with over 90% accuracy, highlighting the effectiveness of shallow feature- based models for real-time applications.

Manuel Sa´nchez-Paniagua et al. [3] presented a real-case phishing detection system that considers login URL structures, domain information, and host-based features, achieving nearly 99% accuracy using Kaggle datasets.

B. Browser Extension Based Detection

M.Amir Syafiq Rohmat Rose et al. [4] implemented a Chrome extension combining machine learning with heuristic rules, achieving 85% accuracy and a precision of 87%. Their work demonstrated the feasibility of integrating phishing de- tection directly into the browser environment.

C. Graph Mining Approaches

Zou Futai et al. [5] proposed a graph mining-based phishing detection method that models user browsing behavior as an AD-URL graph. Although accurate, graph-based approaches are resource-intensive and require large datasets from ISPs.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 03 , March - 2026

D. Pandemic-Driven Threat Landscape

M. Hijji and G. Alam [6] highlighted the rise of phishing at- tacks during the COVID-19 pandemic. Their study emphasized the need for adaptive models to address evolving phishing tactics exploiting global crises.

III. PROPOSED SYSTEM

A. System Overview

The proposed system is designed to provide seamless, real- time phishing detection during web browsing sessions. Unlike traditional antivirus or network-level solutions, this system operates directly within the browser, allowing immediate in- terception of suspicious URLs before any sensitive data is submitted.

The core component is a Google Chrome extension built using Manifest V3 specifications. The extension integrates a lightweight, client-side phishing detection model that operates without needing a continuous internet connection for model queries, making it efficient for real-world usage.

Upon visiting a website, the extension performs the follow- ing operations:

1) **Feature Extraction:** The extension extracts features from the URL, domain information, and page content through the browser's Document Object Model (DOM). This includes identifying patterns like IP addresses in URLs, checking for abnormal URL lengths, analyzing form actions, and inspecting embedded scripts.
2) **Real-Time Classification:** The extracted features are fed into a pre-trained Random Forest classifier embed- ded directly in the extension as a JavaScript function using hardcoded decision thresholds. The model outputs a binary decision: phishing or benign.
3) **User Alert:** Based on the classification result, the exten- sion triggers an immediate browser alert. For phishing websites, a warning popup is displayed, advising the user to avoid interacting with the page. For benign websites, an informational message may confirm safety.
4) **No Data Leakage:** All computations occur locally within the browser. No user data, URLs, or browsing history is sent to any external server, ensuring full privacy and compliance with user security standards.

The system architecture consists of content scripts, a back- ground service worker (for setup and event management), and the classifier logic. Since phishing detection is time-sensitive, the system is optimized for low-latency execution. The average decision time per website visit is less than 500 milliseconds, ensuring that the user experience is unaffected.

The solution is designed to be modular and scalable, al- lowing future integration with backend services for updating models, collecting phishing statistics, or deploying advanced detection methods such as deep learning-based URL embed- dings.

B. Feature Extraction

Features are divided into three categories:

1) Address Bar-Based Features:

- **Presence of IP Address:** URLs containing IP addresses are suspicious.
- **URL Length:** Long URLs may hide malicious parts.
- **Special Characters:** Use of '@' and '-' are often indi- cators of phishing.
- **Multiple Subdomains:** Excessive subdomains suggest fraudulent redirection.

2) Domain-Based Features:

- **Domain Age:** Recently registered domains are more likely to be phishing.
- **DNS Record Analysis:** Invalid or missing DNS records are suspicious.
- **Traffic Rank:** Low-ranked websites have higher phishing probabilities.

3) HTML and JavaScript-Based Features:

- **Iframe Usage:** Hidden iframes can mask malicious con- tent.
- **External Resources:** Loading scripts from unknown domains is risky.
- **Form Actions:** Forms submitting data to unrelated do- mains are phishing indicators.

C. Machine Learning Model

The Random Forest classifier is chosen for its ensemble learning capability, combining multiple decision trees to im- prove accuracy and reduce overfitting. It is computationally efficient, making it suitable for browser-based applications.

$$H(x) = \text{MajorityVote}\{h_1(x), h_2(x), ..., h_n(x)\} \quad (1)$$

where

D. System Architecture

Fig. 1 illustrates the architecture of the proposed system.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 03 , March - 2026

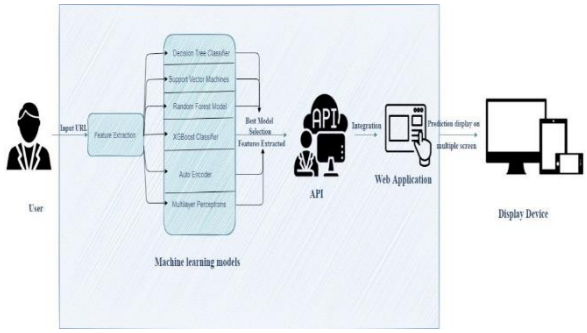

Fig. 1. System Architecture for Phishing Detection Chrome Extension.

IV. IMPLEMENTATION

A. Dataset

A dataset of 6,000 URLs was used, comprising phishing websites from PhishTank and benign websites from trusted sources like the University of New Brunswick. The dataset was split 70% for training and 30% for testing.

B. Model Training and Testing

Several algorithms were tested: Decision Trees, SVM, XG- Boost, Neural Networks, and Random Forest. Table I presents the results.

C. Real-World Deployment

The model was integrated into a Chrome extension using JavaScript and Manifest V3 specifications. The content script extracts features and runs the prediction in real-time. Alerts are displayed via browser pop-ups when phishing is detected.

TABLE I
MODEL PERFORMANCE COMPARISON

Model	Acc.	Prec.	Recall	F1	Spec.
SVM	82.57%	75.2%	97.06%	84.6%	68.13%
XGBoost	86.13%	81.43%	93.52%	87.01%	78.77%
Random Forest	**86.1%**	**81.65%**	**93.05%**	**87.02%**	**79.1%**
Neural Net	82.6%	75.46%	96.59%	84.7%	68.69%
Decision Tree	81.43%	74.5%	95.5%	83.6%	67.5%

V. RESULTS AND DISCUSSION

The proposed phishing detection system was evaluated using a dataset of 6,000 websites, including both malicious and benign URLs. The dataset was divided into 70% for training and 30% for testing to ensure unbiased evaluation.

A. Performance Metrics

The following performance metrics were computed to eval- uate the effectiveness of the classifier:

- **Accuracy:** Proportion of correctly classified instances.
- **Precision:** Proportion of predicted phishing websites that were actually phishing.
- **Recall (Sensitivity):** Proportion of actual phishing web- sites correctly identified.
- **Specificity:** Proportion of benign websites correctly clas- sified.
- **F1-Score:** Harmonic mean of precision and recall.

B. Experimental Results

Table I summarizes the experimental results for differ- ent machine learning algorithms. The Random Forest model achieved the best balance of accuracy, recall, and precision, making it suitable for real-time deployment.

The Random Forest achieved an accuracy of 86.1%, with a high recall of 93.05%, ensuring that most phishing websites are detected. The precision of 81.65% indicates that false positives are reasonably low. A specificity of 79.1% confirms that benign websites are not excessively flagged, maintaining user trust.

C. Real-World Browser Testing

The Chrome extension was deployed and tested in various real-world browsing scenarios. Popular legitimate websites such as *https://www.amazon.com* and *https://www.wikipedia.org* were correctly identified as benign, whereas known phishing test pages were successfully flagged with alerts.

Screenshots were taken during these tests to validate the extension's functionality. The extension consistently displayed warning popups for phishing sites and informational messages for safe websites, as intended.

D. Execution Time and Latency

One of the critical aspects of browser-based security solu- tions is execution time. The extension was tested for latency, and the average detection time per website was measured to be less than 500 milliseconds. This ensures that user experience is not disrupted during browsing.

E. Error Analysis

Some false positives were observed in cases where new or less popular domains had unusual URL structures but were not phishing. These cases are acceptable in practice because a cautious warning is preferable to missing a phishing attempt. False negatives were minimal due to comprehensive feature extraction. However, highly obfuscated phishing websites that closely mimic legitimate URLs might still evade detection. Fu- ture work will focus on reducing these cases by incorporating advanced behavioral analysis.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 03 , March - 2026

F. Comparison with Existing Solutions

Compared to blacklist-based approaches, this system detects zero-day phishing attacks without relying on pre-existing databases. Additionally, unlike server-side models, the browser extension operates locally, maintaining user privacy and reduc- ing response time.

G. User Experience

The simplicity of the alert system ensures that users receive clear and actionable feedback. No additional configuration is required from the user, making the solution accessible to non- technical individuals.

Overall, the results demonstrate that the proposed system is effective, practical, and deployable for real-time phishing detection in modern web browsers.

VI. CONCLUSION AND FUTURE WORK

This paper presents a practical, real-time phishing detection system implemented as a Google Chrome browser exten- sion. The system uses a Random Forest classifier trained on a comprehensive feature set including URL-based, domain- based, and HTML/JavaScript-based attributes. The results demonstrate that the proposed model achieves high detection accuracy, with an emphasis on minimizing false positives while maintaining a high phishing detection rate.

The main contributions of this work include:

- Development of a lightweight machine learning model suitable for browser-based deployment.
- Integration of phishing detection into a Chrome extension without affecting user browsing experience.
- Real-time alert system with immediate feedback to end- users.
- Preservation of user privacy, as no data is sent to external servers.

The experimental results validate the model's robustness, with an accuracy of 86.1%, a precision of 81.65%, and a recall of 93.05%. The system successfully detects both known and zero-day phishing attempts, offering proactive protection.

A. Future Work

While the current system performs effectively, several en- hancements are planned for future research and development:

- **Cross-Browser Deployment:** Extend support to other browsers such as Mozilla Firefox, Microsoft Edge, and Opera to increase user reach.
- **Deep Learning Integration:** Incorporate deep learning models, such as LSTM or Transformer-based URL embeddings, for improved detection of obfuscated phishing URLs.
- **Backend Threat Intelligence:** Implement a cloud-based backend for model updates and collaborative phishing URL reporting, allowing the system to adapt to emerging threats.
- **User Feedback Loop:** Enable users to provide feedback on false positives or missed phishing attempts, facilitating incremental model improvement.
- **Behavioral Analysis:** Include analysis of website behavior, such as mouse tracking or time-to-first-click metrics, to identify suspicious user interaction patterns.
- **Mobile Browser Support:** Develop a version of the extension compatible with mobile browsers to protect users on smartphones and tablets.

These future directions aim to create a more robust, adap- tive, and user-friendly phishing detection ecosystem, address- ing the continuously evolving landscape of cyber threats.

REFERENCES

[1] A. Mandadi, S. Boppana, V. Ravella, and R. Kavitha, "Phishing Website Detection Using Machine Learning," in Proc. IEEE, 2022.

[2] A. N. Soma Charan, Y.-H. Chen, and J.-L. Chen, "Phishing Websites Detection using Machine Learning with URL Analysis," in Proc. IEEE World Conference on Applied Intelligence and Computing, 2022.

[3] M. Sa´nchez-Paniagua, E. Fidalgo Ferna´ndez, E. Alegre, W. AlNabki, and

V. Gonza´lez-Castro, "Phishing URL Detection: A Real-Case Scenario Through Login URLs," in Proc. IEEE, 2022.

[4] M. A. S. R. Rose, N. Basir, N. F. N. R. Heng, N. J. M. Zaizi, and M. M. Saudi, "Phishing Detection and Prevention using Chrome Extension," in Proc. IEEE, 2022.

[5] F. Zou, Y. Gang, B. Pei, L. Pan, and L. Linsen, "Web Phishing Detection Based on Graph Mining," in Proc. IEEE, 2016.

[6] M. Hijji and G. Alam, "A Multivocal Literature Review on Growing Social Engineering Based Cyber-Attacks/Threats During the COVID-19 Pandemic: Challenges and Prospective Solutions," in Proc. IEEE, 2021.

[7] PhishTank, "PhishTank Phishing Data Archive," [Online]. Available: https://www.phishtank.com/

[8] University of New Brunswick, "Phishing and Legitimate URL Dataset," [Online]. Available: https://www.unb.ca/cic/datasets/phishing.html

[9] Google Safe Browsing, "Google Transparency Report," [Online]. Avail- able: https://transparencyreport.google.com/safe-browsing

(This work is licensed under a Creative Commons Attribution 4.0 International License.)