International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2025.0168
e ISSN: 2584-2854
Volume: 03
Issue:04 April 2025
Page No: 1029 - 1034

Phishing Attack Stimulation and Prevention Mechanism

Karthikeyan C[1], Mugilan M[2], Nithish S[3], Ranjithkumar S[4], Abinesh M[5]
[1]Professor, Dept. of IT, Erode Sengunthar Engineering College, Erode, Tamil Nadu, India.
[2,3,4,5]UG Scholar, Dept. of IT, Erode Sengunthar Engineering College, Erode, Tamil Nadu, India.
Email ID: *mugilan359389@gmail.com[1], nk5588678@gmail.com[2], ranjithsivalingam28@gmail.com[3], abinesh07042004@gmail.com[4]*

Abstract
Phishing attacks have become one of the most prevalent cyber security threats, exploiting social engineering techniques to deceive users into revealing sensitive information such as passwords, banking details, and personal data. Cybercriminals continuously refine their tactics, making traditional security measures like blacklists and rule-based filters less effective. To address this challenge, we propose a machine learning (ML)–based browser extension designed to detect and prevent phishing attempts in real-time. Initially developed for Google Chrome but adaptable to other browsers, the extension operates in persistent "pin mode", ensuring continuous monitoring of URLs entered by users. By extracting key features such as domain attributes, SSL certificate details, URL structure, and lexical patterns, the extension employs a trained ML model to accurately classify web pages as legitimate or potentially malicious. When a phishing attempt is detected, the extension immediately alerts the user with warnings, preventing them from interacting with fraudulent sites. This solution outperforms traditional blacklist-based approaches by leveraging AI to detect emerging threats, making it more robust against evolving phishing techniques. Additionally, the extension is designed to be lightweight and user-friendly, ensuring it does not compromise browser performance while providing seamless, proactive protection against online scams. Future enhancements could incorporate behavioral analysis, adaptive learning techniques, and integration with external threat intelligence feeds to further improve detection accuracy and resilience against new phishing strategies.

Keywords: *Phishing attacks, Cybersecurity threats, Social engineering, Sensitive information, Machine learning (ML), Browser extension, Real-time detection, Google Chrome, Persistent monitoring*

1. Introduction
Phishing attacks have become one of the most widespread cybersecurity threats, using deceptive tactics and social engineering techniques to manipulate users into revealing sensitive information such as passwords, banking credentials, and personal data. Cybercriminals increasingly employ sophisticated strategies, including website spoofing, URL obfuscation, and dynamic content manipulation, making it difficult for traditional security mechanisms like blacklists and rule-based filters to detect emerging threats effectively. To address these challenges, this project proposes a machine learning (ML)–based browser extension that provides real-time phishing detection and prevention. Initially developed for Google Chrome but adaptable to other browsers, the extension operates in persistent "pin mode", ensuring continuous monitoring of every URL entered by the user. By leveraging advanced ML algorithms, the system analyzes various features of a URL, such as domain attributes, SSL certificate details, URL length, the presence of special characters, and lexical patterns, to accurately classify web pages as safe or potentially malicious. When a phishing attempt is detected, the extension instantly warns the user, preventing interaction with fraudulent websites and mitigating the risk of credential theft. Unlike conventional security solutions that rely on static blacklists, this ML-based approach offers

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2025.0168
e ISSN: 2584-2854
Volume: 03
Issue:04 April 2025
Page No: 1029 - 1034

greater adaptability and resilience, allowing it to detect newly emerging threats without requiring manual updates. The extension is designed to be lightweight, efficient, and user-friendly, ensuring minimal impact on browser performance while providing seamless, real-time protection. Future enhancements may include behavioral analysis, adaptive learning techniques, and integration with external cyber security intelligence sources to further improve detection accuracy and strengthen defenses against evolving phishing tactics. By leveraging artificial intelligence, this project aims to provide a robust, automated, and intelligent solution for combating phishing attacks, ensuring users can browse the internet safely and securely. [1]

2. Literature Survey

Phishing remains a significant cybersecurity challenge, with attackers continually refining their techniques to exploit user vulnerabilities. Various detection and prevention strategies have been developed, ranging from community-driven databases to advanced artificial intelligence (AI)-based models. PhishTank is a user-driven phishing detection system that allows individuals to report and verify phishing websites, creating a publicly accessible database of fraudulent sites. This crowd-sourced approach improves phishing detection but relies on user submissions, leading to potential delays in identifying new threats [1]. DeepPhish utilizes Convolutional Neural Networks (CNNs) to analyze the visual appearance of websites, detecting phishing attempts based on graphical similarities to legitimate sites. This method is highly effective against phishing attempts that mimic well-known brands but requires substantial computational resources and may struggle with dynamically changing phishing sites [2]. AntiPhish, a browser extension, monitors user interactions to prevent credential theft. It alerts users if their login credentials are entered on potentially fraudulent websites. Although this real-time protection enhances security, it does not cover phishing attacks conducted via email, SMS, or other non-web-based vectors [3]. A hybrid phishing detection system integrates heuristic-based analysis with machine learning models to improve detection accuracy. The heuristic approach identifies suspicious domain names, misleading links, and urgent language, while machine learning algorithms enhance adaptability to evolving phishing tactics. However, this method requires continuous updates and retraining to maintain effectiveness against new threats [4]. Natural Language Processing (NLP) techniques have been employed to analyze phishing emails by detecting suspicious language patterns, urgency-driven messages, and financial baiting tactics. While NLP-based phishing detection improves classification accuracy, it can produce false positives, flagging legitimate emails as malicious due to overlapping linguistic characteristics [5]. An image-based phishing detection system applies computer vision techniques to analyze webpage screenshots and compare them against known legitimate websites. This method is particularly effective against phishing sites that visually replicate trusted brands. However, its high computational cost and susceptibility to adversarial modifications remain challenges [6]. Multi-Factor Authentication (MFA) strengthens security by requiring users to verify their identity through multiple authentication factors, such as one-time passwords or biometric verification. While MFA significantly reduces phishing risks, advanced phishing techniques, such as adversary-in-the-middle (AitM) attacks, attempt to bypass these security measures, highlighting the need for more robust authentication solutions [7]. The reviewed literature demonstrates that phishing detection and prevention require a multi-layered approach. While traditional blacklist-based methods struggle to keep up with evolving threats, AI-driven techniques, behavioral monitoring, and community-based reporting offer more effective solutions. Future research should focus on integrating these approaches to develop a more resilient anti-phishing framework.

3. Proposed System

The proposed system is an advanced browser extension that leverages machine learning to detect and prevent phishing attacks in real-time. Unlike traditional blacklist-based or rule-driven methods, this extension analyzes each URL dynamically using AI-powered classification to identify potential threats, even when facing newly emerging or zero-day phishing websites. When users enter a URL, click

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2025.0168
e ISSN: 2584-2854
Volume: 03
Issue:04 April 2025
Page No: 1029 - 1034

on a link, or are redirected to a new page, the extension immediately intercepts the request and performs in-depth feature extraction. It evaluates attributes such as domain structure, SSL certificates, lexical patterns, and other phishing indicators. This data is processed by a pre-trained ML model, which assigns a phishing likelihood score to determine if the website is safe or malicious. If a URL is deemed suspicious, the system automatically triggers visual, audio, or pop-up alerts, and may block access to the site depending on the severity. Designed for accessibility and ease of use, the extension ensures that users receive real-time warnings without any impact on system performance or browsing experience. [2-5]

3.1.Key Features of the Proposed System

- **Real-Time URL Analysis:** Continuously monitors user interactions (typed URLs, clicks, redirects) and evaluates URLs in real-time using machine learning.
- **AI-Based Detection:** Uses a pre-trained machine learning model to assess phishing likelihood based on structural, lexical, and domain-level features.
- **Instant Alerts & Prevention:** Triggers immediate visual pop-ups, banners, and audio warnings for suspicious sites. Supports auto-blocking of high-risk websites.
- **Accessibility Support:** Compatible with screen readers like NVDA, JAWS, and VoiceOver; includes keyboard navigation, high-contrast mode, and customizable fonts.
- **Lightweight & Seamless Integration:** Designed to work efficiently in Google Chrome, Firefox, Microsoft Edge, and other Chromium-based browsers with minimal performance overhead.
- **Adaptive Learning:** Continuously updates its detection capability through user feedback and periodic model retraining to respond to new phishing trends.
- **User Customization:** Allows customization of phishing sensitivity levels, creation of allowlists for trusted websites, and manual reporting of suspicious links.
- **Privacy-Focused Design:** Operates locally where possible and ensures encrypted communication with cloud services; does not collect or store personal data or browsing history.
- **Dynamic Threat Intelligence Integration:** Future support for integration with external blacklists, threat intelligence feeds, and behaviour analysis modules for enhanced detection.
- **Modular Architecture:** Divided into specialized components (URL monitoring, ML classification, alert/prevention, feedback/adaptive learning) to ensure scalability and maintainability.

4. Methodology

4.1. Data Collection and Pre-Processing

The system begins by collecting a large dataset of phishing and legitimate URLs from reliable sources such as Phish Tank, Open Phish, and Alexa Top Sites. This dataset includes multiple attributes like domain names, URL lengths, HTTPS status, SSL certificate information, special character usage, redirection behaviour, and WHOIS registration data. Pre-processing techniques are applied to clean the data by removing duplicates, handling missing values, and normalizing formats. Features are encoded into machine-readable formats using label encoding and one-hot encoding techniques. This ensures consistent and accurate input for training machine learning models.

4.2.Machine Learning Model Implementation

Supervised machine learning algorithms, such as Random Forest, Support Vector Machine (SVM), or Decision Trees, are trained using the preprocessed dataset. These models are fine-tuned to classify URLs based on phishing likelihood. The model analyzes lexical and structural patterns in URLs, SSL certificate details, and other critical attributes. A phishing probability score is generated for each URL, determining whether a website is malicious or legitimate. Model performance is optimized through cross-validation, ensuring high accuracy, low false positive rates, and robust generalization to unseen phishing domains.

4.3.Extension Development and Integration

The phishing detection system is deployed as a The

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2025.0168
e ISSN: 2584-2854
Volume: 03
Issue:04 April 2025
Page No: 1029 - 1034

lightweight browser extension for Google Chrome, with compatibility for other Chromium-based browsers. The extension operates in persistent "pin mode," monitoring user activities such as typing URLs, clicking on links, or being redirected to new pages. On each interaction, the extension extracts feature from the URL and sends them to the embedded machine learning model for evaluation. Based on the phishing likelihood score, the extension provides real-time feedback, either alerting the user or blocking the navigation to ensure online safety.

4.4.User Interface and Alert System

To maximize user accessibility and awareness, the extension includes a multi-modal alert system. Visual warnings, pop-up messages, and audio notifications are triggered when a phishing threat is detected. The UI is designed for inclusivity, supporting screen readers like NVDA, JAWS, and VoiceOver, as well as high-contrast modes and customizable font sizes. Users can also adjust security sensitivity levels and create allowlists for trusted websites, offering a personalized experience.

4.5.Adaptive Learning and Feedback Integration

The system includes mechanisms for adaptive learning through user feedback. When users report false positives or missed phishing threats, this feedback is incorporated into model updates. The learning algorithm periodically retrains using new phishing samples, improving detection accuracy and adapting to evolving phishing strategies. Integration with external threat intelligence feeds is also planned to further enhance threat awareness.

4.6.Real-Time Security Monitoring

The extension continuously monitors URL activity in real time without compromising browser performance. It uses minimal system resources, ensuring a smooth user experience while running in the background. Real-time interception of URLs allows the extension to react instantly, safeguarding users from fraudulent sites that exploit quick decision-making moments.

4.7.Security, Privacy, and Deployment

To maintain user trust, the system is built with strong security and privacy considerations. All data processing is done locally where possible, and any communication with external servers for model inference is encrypted. The extension does not store browsing history or personal data, complying with privacy standards. After iterative testing and optimization, including latency reduction and model efficiency tuning, the system is deployed to ensure reliable phishing protection across different browsing environments. [6-8]

5. Result and Discussion

5.1.Result

The development and testing of the phishing detection browser extension produced accurate, responsive, and reliable results across all core modules, confirming its practical viability and effectiveness in real-time threat detection. Unit testing validated the independent functionality of key modules, including URL Monitoring and Feature Extraction, ML-Based Classification, and Alert and Prevention. Each module operated as intended, with precise feature extraction, accurate phishing prediction, and prompt alert generation. Integration testing further ensured smooth interaction between modules, confirming that extracted URL features were correctly passed to the ML model and that detection results triggered the appropriate user warnings. System testing evaluated the extension's real-time performance during simulated browsing scenarios, confirming that the system successfully intercepted and analyzed URLs without introducing noticeable delays. Additionally, User Acceptance Testing (UAT) demonstrated positive feedback from testers, who appreciated the seamless integration, minimal impact on browser performance, and clear alert notifications. The system consistently detected phishing attempts and blocked access to malicious URLs while maintaining a lightweight and accessible user experience.

5.2.Discussion

The successful testing of the phishing detection browser extension highlights its robustness and efficiency in delivering real-time cybersecurity protection. Unit testing played a key role in ensuring each module met its individual requirements—particularly the accuracy of feature extraction and classification models, which are central to reliable phishing detection. Integration testing revealed

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2025.0168
e ISSN: 2584-2854
Volume: 03
Issue:04 April 2025
Page No: 1029 - 1034

effective data flow between modules, proving the system's ability to deliver accurate and timely responses to potential threats. The system testing phase validated the performance of the extension under various user interaction scenarios, including high-frequency URL requests and redirection chains. The extension maintained a stable performance without impacting browser speed, confirming its readiness for real-world use. UAT provided valuable feedback that helped improve user interaction—such as refining the alert pop-ups and ensuring better screen reader compatibility for visually impaired users. This phase confirmed that the extension met user expectations for usability, speed, and reliability. While the extension has shown strong performance in controlled environments, ongoing monitoring and user feedback will be essential for continued improvement, especially as phishing tactics evolve. Future updates will focus on enhancing adaptive learning, refining phishing detection thresholds, and integrating additional threat intelligence sources to maintain high detection accuracy over time.

Conclusion

The phishing detection browser extension developed in this project provides a robust, intelligent, and user-friendly solution to one of the most persistent cybersecurity threats—phishing attacks. By leveraging machine learning algorithms, the system is capable of accurately identifying malicious URLs in real time, significantly outperforming traditional blacklist and rule-based detection methods. Through effective feature extraction, real-time monitoring, and adaptive learning, the extension ensures users are proactively alerted to potential threats without compromising browsing speed or user experience. The modular architecture and privacy-focused design further enhance its efficiency, scalability, and trustworthiness. Extensive testing, including unit, integration, system, and user acceptance testing, has confirmed the extension's stability, accuracy, and ease of use. Positive feedback from users highlights the system's accessibility, lightweight performance, and effectiveness in providing real-time protection. As phishing techniques continue to evolve, this solution lays a strong foundation for future enhancements, such as behavioral analysis, external threat intelligence integration, and dynamic model retraining. Overall, the project demonstrates the power of artificial intelligence in strengthening web security and provides a practical tool for protecting users from online scams and cyber threats.

Reference

[1]. Lakshmanarao, A., Rae, P.S.P., Krishna, M.M.B. (2021) 'Phishing website detection using novel machine learning fusion approach', in 2021 International Conference on Artificial Intelligence and Smart Systems (ICAIS), Presented at the 2021 International Conference on Artificial Intelligence and Smart Systems (ICAIS), 1164–1169

[2]. H. Chapala, R. Kodak and M. Joiner, "A Machine Learning Approach for URL Based Web Phishing Using Fuzzy Logic as Classifier", 2019 International Conference on Communication and Electronics Systems (ICCES), pp. 383-388, 2019, July

[3]. Vaishnavi, D., Sabetha, S., Jingle, Y.B., Submachine, R., Shyly, S.P. (2021) 'A Comparative Analysis of Machine Learning Algorithms on Malicious URLPrediction', in20215thInternationalConferenceonIntelligentComputingandControl Systems (ICICCS), Presented at the 2021 5th International Conference on Intelligent Computing and Control Systems (ICICCS), 1398–1402

[4]. Internal Revenue Service, IRS E-mail Schemes. Available at https:// www.irs.gov/ uac/newsroom/consumers-warnedof-new-surge-in-irs-email-schem es-during-2016-tax-season-tax-industry-also-targeted.

[5]. Abu-Nimes, S., Napa, D., Wang, X., Nair, S. (2007), A comparison of machine learning techniques for phishing detection.

[6]. E., B., K., T. (2015). Phishing URL Detection: A Machine Learning and Web Mining-based Approach. International Journal of Computer Applications, 123(13), 46-50.doi:10.5120/ijca2015905665.

[7]. Wang Wei-Hong, LVY in-Jun, CHEN Hui-Bing, FANG Zhao-Lin., A Static Malicious Java script Detection Using SVM, In Proceedings of the 2nd International

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2025.0168
e ISSN: 2584-2854
Volume: 03
Issue:04 April 2025
Page No: 1029 - 1034

Conference on Computer Science and Electrical Engineering (ICCSEE 2013).

[8]. Ningxia Zhang, Youngling Yuan, Phishing Detection Using Neural Net-work, In Proceedings of International Conference on Neural Information Processing, pp. 714–719. Springer, Heidelberg (2004)