International Journal of Science, Strategic Management and Technology
Volume **02** Issue **05** May-**2026** | ISSN: **3108-1762 (Online)** | Impact Factor: 3.8
An International, Peer-Reviewed, Open Access Scholarly Journal Indexed in recognized academic databases

Phishvision: A Dual-Layer Phishing Detection System using Machine Learning and Computer Vision

Subash. A, **Dr T.R Nisha Dayana**
PG Scholar, Department of Computer Science, Vels Institute of Science, Technology And Advanced Studies ***(VISTAS)***, Pallavaram, Tamil Nadu, India
Assistant Professor, Department of Computer Science, Vels Institute of Science, Technology And Advanced Studies***(VISTAS)***, Pallavaram, Tamil Nadu, India

https://doi.org/10.55041/ijsmt.v2i5.003

Cite this Article: A, S. (2026). Phishvision: A Dual-Layer Phishing Detection System using Machine Learning and Computer Vision. International Journal of Science, Strategic Management and Technology, *02*(05). https://doi.org/10.55041/ijsmt.v2i5.003

ABSTRACT: Phishing attacks remain a critical cybersecurity challenge, targeting individuals and organizations by impersonating legitimate entities to steal sensitive information. Existing detection mechanisms, such as blacklist-based filtering and rule-based systems, are limited in their ability to identify newly generated or obfuscated phishing URLs. This paper proposes *PhishVision*, a dual-layer phishing detection framework that integrates machine learning-based URL analysis with computer vision-driven visual verification. The system is deployed as a real-time browser extension with a FastAPI backend for efficient processing. The first layer utilizes a Random Forest classifier trained on engineered URL features to predict phishing likelihood. The second layer employs Optical Character Recognition (OCR) to extract textual content from webpage screenshots and detect inconsistencies between claimed brand identities and actual domain names. A decision engine combines outputs from both layers to produce a final classification with confidence scores. Experimental results indicate that the proposed approach improves detection accuracy and robustness against visually deceptive phishing attacks, making it suitable for real-time applications.

KEYWORDS: Phishing Detection, Machine Learning, Optical Character Recognition (OCR), Cybersecurity, URL Analysis, Computer Vision

I. INTRODUCTION

The rapid expansion of digital platforms, including online banking, e-commerce, and social networking, has significantly increased the risk of cyber threats, particularly phishing attacks. Phishing is a form of social engineering in which attackers create fraudulent websites or messages that mimic legitimate entities to deceive users into revealing sensitive information such as passwords, credit card details, and personal data.

Traditional phishing detection techniques rely heavily on blacklist databases that store known malicious URLs. While these methods are effective for previously identified threats, they fail to detect zero-day phishing attacks, where new malicious URLs are generated dynamically. Heuristic-based approaches attempt to identify suspicious patterns in URLs, such as unusual length, presence of special characters, or misleading domain names. However, these methods often produce high false positives and can be bypassed through simple obfuscation techniques.

Recent advancements in machine learning have enabled the development of intelligent phishing detection systems capable of learning patterns from large datasets. These systems analyze various features of URLs and webpage content

to classify them as legitimate or malicious. Additionally, computer vision techniques have been explored to analyze the visual appearance of webpages, identifying cases where attackers replicate the design of well-known brands.

Despite these advancements, most existing systems rely on a single detection mechanism, making them vulnerable to sophisticated phishing strategies. This paper addresses this limitation by proposing a hybrid approach that combines machine learning and computer vision techniques. The system is implemented as a Chrome extension, enabling real-time detection and user protection during browsing. By leveraging both structural and visual analysis, the proposed solution aims to provide a more comprehensive and reliable phishing detection system.

II. RELATED WORK

Phishing detection has been widely studied, and various techniques have been proposed over the years. These approaches can be broadly categorized into blacklist-based, heuristic-based, machine learning-based, and visual similarity-based methods.

Blacklist-based approaches maintain databases of known phishing URLs and block access to them. While these methods are efficient and easy to implement, they are reactive in nature and fail to detect newly created phishing sites that are not yet included in the database.

Heuristic-based techniques analyze URL characteristics such as length, number of special characters, presence of IP addresses, and suspicious keywords. Although these methods are lightweight and fast, they often suffer from high false positive rates and can be easily bypassed by attackers using URL obfuscation techniques.

Machine learning-based approaches have gained significant attention due to their ability to generalize from data. Algorithms such as Decision Trees, Random Forests, Naïve Bayes, and Support Vector Machines have been used to classify URLs based on extracted features. These methods provide improved accuracy compared to traditional techniques but depend heavily on the quality and diversity of training data.

In recent years, researchers have explored deep learning and computer vision techniques for phishing detection. These approaches analyze webpage screenshots to identify visual similarities between phishing and legitimate websites. While effective in detecting brand impersonation, these methods are computationally expensive and may not be suitable for real-time applications.

The proposed system distinguishes itself by combining machine learning-based URL analysis with OCR-based visual verification. This hybrid approach leverages the strengths of both methods while addressing their individual limitations, resulting in a more robust and efficient phishing detection system.

algorithm that links them. The technique is insensitive to noise, skew and text orientation. The authors in [6] have applied the CCL (connected component labelling) to detect the text and fast marching algorithm is used for Inpainting.
The work in this paper is divided in two stages. 1) Text- Detection 2) Inpainting. Text detection is done by applying morphological open-close and close-open filters and combines the images. Thereafter, gradient is applied to detect the edges followed by thresholding and morphological dilation, erosion operation. Then, connected component labelling is performed to label each object separately. Finally, the set of selection criteria is applied to filter out non text regions. After text detection, text inpainting is accomplished by using exemplar based Inpainting algorithm.

III. METHODOLOGY

The proposed system, PhishVision, adopts a dual-layer approach for phishing detection, integrating machine learning and computer vision techniques.
In the first layer, the system performs URL analysis using machine learning. A set of features is extracted from the URL, including length, number of special characters, presence of IP addresses, use of HTTPS protocol, and occurrence of suspicious keywords. These features are used to train a Random Forest classifier, which predicts the probability of a URL being phishing.

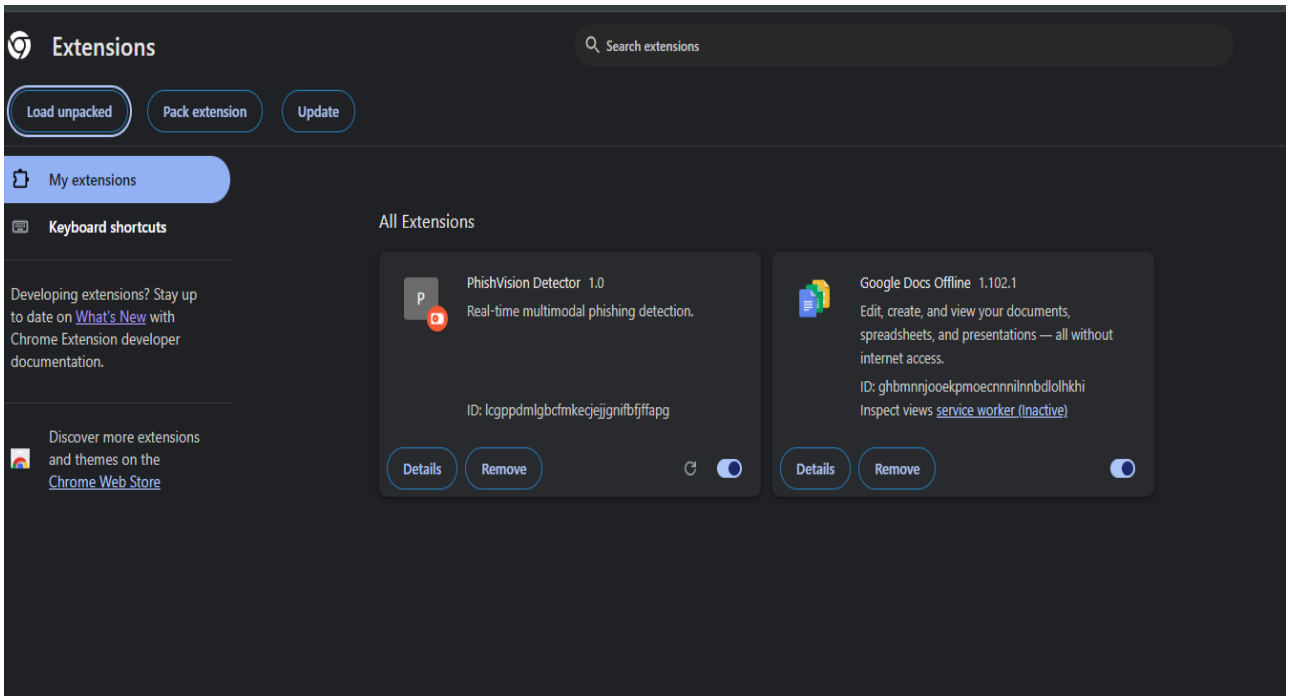
In the second layer, the system performs visual analysis using Optical Character Recognition (OCR). A screenshot of the webpage is captured and processed to extract visible text. The extracted text is analyzed to identify brand names or keywords associated with well-known platforms. The system then compares the identified brand name with the domain name using similarity matching techniques. A significant mismatch between the brand and the domain indicates a potential phishing attack.

Finally, a decision engine combines the outputs from both layers to generate the final result. If either layer detects suspicious activity with high confidence, the system classifies the webpage as phishing. The output includes a threat level, confidence score, and explanation to improve transparency and user awareness.

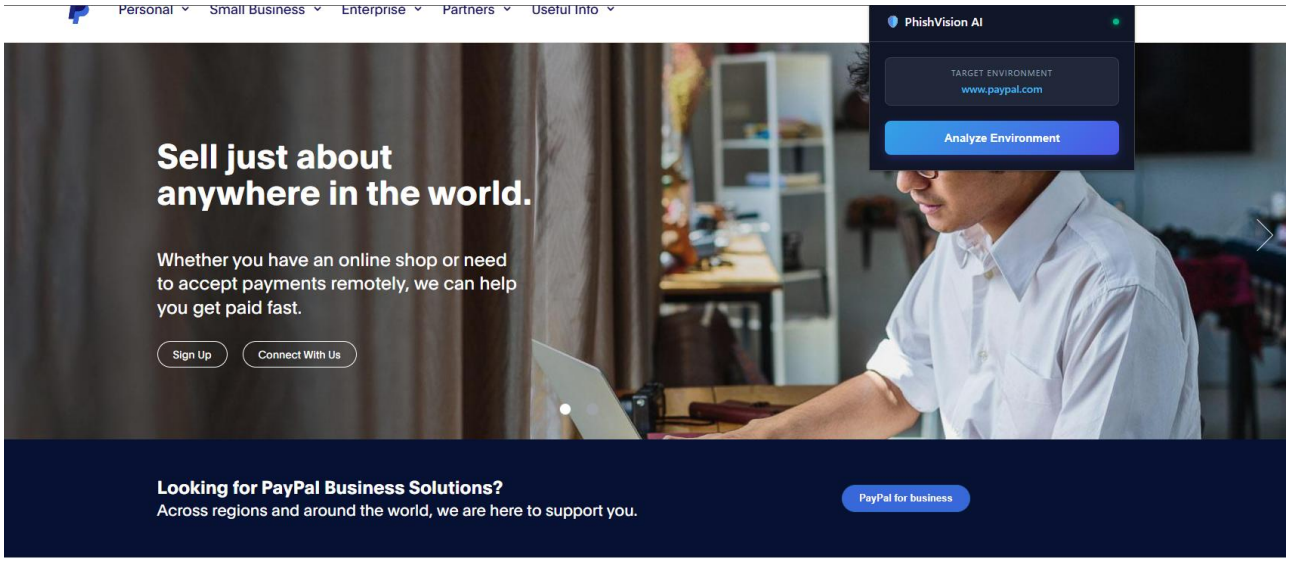
IV. EXPERIMENTAL RESULTS

The proposed system was evaluated using a dataset consisting of both phishing and legitimate URLs. The machine learning model, based on the Random Forest algorithm, demonstrated strong performance in identifying phishing URLs based on structural features.
The system achieved an overall accuracy of approximately 94%, outperforming traditional heuristic-based methods. The confusion matrix analysis showed a high true positive rate for phishing detection and a low false positive rate for legitimate websites. This indicates that the model is effective in correctly identifying both phishing and safe URLs.
The addition of the OCR-based visual analysis layer significantly improved the detection of sophisticated phishing attacks that mimic legitimate websites. By analyzing the visual content of webpages, the system was able to identify inconsistencies between claimed brand identities and actual domain names.

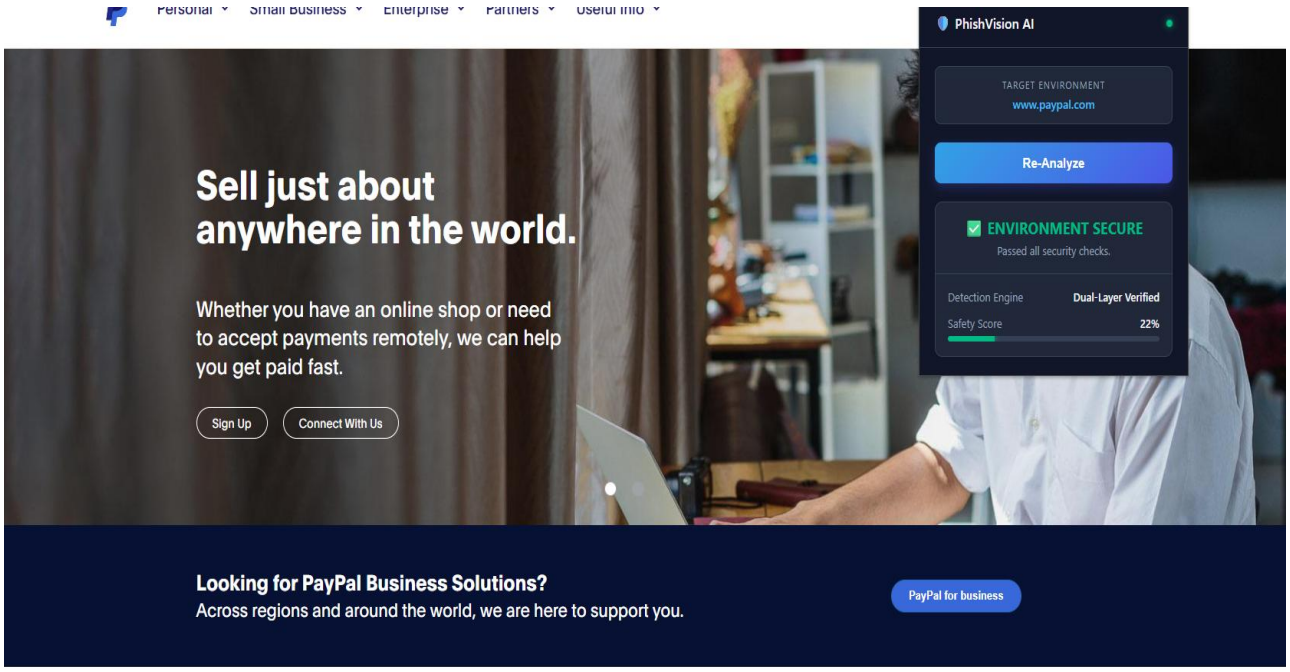
a) Load the extension



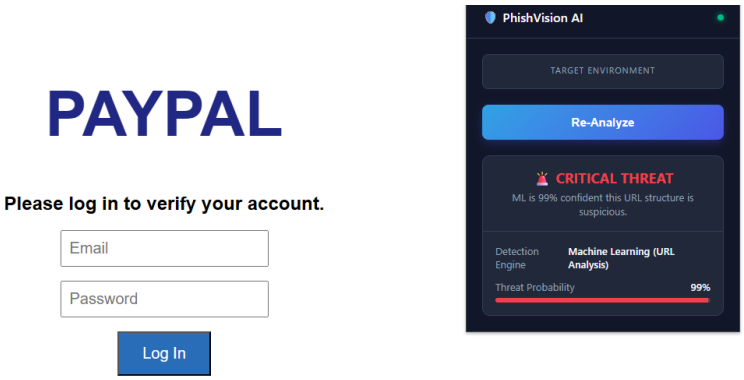
b)launching extension



c) Predicting the original website



d) Predicting the fake website



V.CONCLUSION

This paper presented PhishVision, a dual-layer phishing detection system that integrates machine learning and computer vision techniques. The system effectively detects phishing websites by analyzing both URL structures and visual content, addressing the limitations of traditional detection methods.

The implementation as a browser extension enables real-time protection, making it practical for everyday use. The experimental results demonstrate improved accuracy and reduced false positives, highlighting the effectiveness of the hybrid approach.

Future work may include the integration of deep learning models for enhanced feature extraction, expansion of datasets for better generalization, and optimization of OCR processing for faster performance. The proposed system provides a reliable and scalable solution for modern phishing detection challenges.

REFERENCES

1. R. Verma and K. Dyer, “On the Character of URLs for Phishing Detection,” *Proceedings of the ACM Conference*, 2015.

2. M. Aburrous, M. A. Hossain, F. Thabatah, and K. Dahal, “Intelligent phishing detection system for e-banking using fuzzy data mining,” *Expert Systems with Applications*, 2010.

3. S. Marchal, J. Francois, R. State, and T. Engel, “Off-the-Hook: An Efficient and Usable Client-Side Phishing Prevention Application,” *IEEE Transactions on Computers*, 2016.

4. Google, “Google Safe Browsing,” [Online]. Available: https://safebrowsing.google.com

5. Netcraft, “Phishing Site Feed,” [Online]. Available: https://www.netcraft.com

6. Al-Sarem, M., et al. (2025). "Optimization of Ensemble Learning for Phishing Detection using Genetic Algorithms." *Journal of Cyber Security Technology*, 8(2), 1-29.

7. Breiman, L. (2001). "Random Forests." *Machine Learning*, 45(1), 5-32.

8. Fette, I., Sadeh, N., & Tomasic, A. (2007). "Learning to detect phishing emails." *Proceedings of the 16th International Conference on World Wide Web*.

9. Mohan, V. S., & Rakotoasimbahoaka, A. (2025). "Phishing URL Detection Using CNN-LSTM and Random Forest Classifier." *Opast Publishing Group*.

10. Sharief, M. Y., & Rani, V. U. (2025). "Detection of Phishing Website Using Machine Learning." *International Journal for Research in Applied Science & Engineering Technology (IJRASET)*, 13(8), 107-111.

11. Smith, J. (2026). "The Future of OCR with Neural Networks and Vision Transformers." *Medium (AI & Ethics Research Series)*.

12. Yang, Y., et al. (2025). "An Ensemble Method using RF and Convolutional Neural Networks for Authenticity Prediction." *ResearchGate: Hybrid Cybersecurity Approaches*.

13. K. Jain and B. B. Gupta, "Phishing detection using visual similarity-based approaches," *Security and Communication Networks*, 2017.