ISSN 2319-5991 www.ijerst.com
© 2026 IJERST. All Rights Reserved
Peer Reviewed, Referred & Indexed Journal

Research Paper

Real-Time Ai/Ml Based Phishing Detection and Prevention System

[1]V. Prasad, [2]P. Srija, [3]M. Sahithi, [4]Ch. Naga Shreya,[5]P. Pujitha

[1]Assistant Professor, Dept of CSE-AI&ML, St. Ann's College of Engineering and Technology Chirala-523187, India.

[2,3,4,5]U. G Student, Dept of CSE-AI&ML, St. Ann's College of Engineering and Technology Chirala-523187, India.

ABSTRACT- ***Phishing attacks have become one of the most common widespread cybersecurity threats, targeting individuals and organizations through malicious websites, emails, and fake URLs. Traditional phishing detection techniques mainly rely on blacklist databases and manually define rules, which often fail to identify newly emerging phishing websites. This research presents a Real-Time AI/ML Based Phishing Detection and Prevention System that utilizes Machine Learning algorithms to accurately distinguish between legitimate and phishing URLs. The proposed system extracts important URL-based features, including URl length, special characters, HTTPS usage, subdomain count, IP address presence, and digit frequency, to classify websites effectively. A Random Forest classifier is trained on a phishing dataset to provide fast and reliable predictions. The system is integrated with a user-friendly web interface that enables real-time URL analysis and instant threat alerts. Experimental results demonstrate high detection accuracy and efficient performance, making the proposed solution suitable for practical cybersecurity applications.***

KEYWORDS: ***Phishing Detection, Machine Learning, Random Forest Classifier, URL Feature Extraction, Cybersecurity.***

INTRODUCTION

The rapid growth of internet services and online transactions has significantly increased the number of phishing attacks worldwide. Cybercriminals crate fake websites that imitate trusted organizations to steal sensitive information such as usernames, passwords, banking credentials, and personal data. Conventional phishing detection methods depend on manually updated blacklist predefined security rules, which cannot effectively detect newly created phishing websites. Artificial Intelligence and Machine Learning have emerged as powerful solutions for identifying phishing attacks through intelligent pattern recognition. Machine learning models can automatically learn distinguishing characteristics from large datasets without requiring constant manual updates. The proposed Real-Time AI/ML Based Phishing Detection and Prevention System applies feature extraction and

Random Forest classification to detect phishing URLs accurately while providing immediate feedback to users. This intelligent approach online security by preventing users from accessing malicious websites before sensitive information is compromised.

LITERATURE SURVEY

Numerous researches have investigated phishing detection using machine learning and artificial intelligence techniques. Early approaches relied on blacklist verification, heuristic analysis, and manually engineered security rules, which showed limited effectiveness against newly generated phishing websites. Later studies introduced supervised learning algorithms such as Decision tress, Navie Bayes, Support Vector Machines, and Random Forests to classify URLs based on extracted features. Deep Learning techniques have also been explored for automatically learning phishing patterns from large datasets. Although these methods improved detection accuracy, many existing systems require extensive computational resources or fail to perform efficiently in real-time environments. Therefore, developing a lightweight, accurate, and real-time phishing detection framework remains an important research objective.

RELATED WORK

Several phishing detection systems have utilized artificial intelligence to improve cybersecurity. Researches have proposed URL-based classification models using lexical feature extraction combined with machine learning algorithms. Other studies have focused on webpage content analysis, domain reputation, visual similarity detection, and browser extensions for phishing prevention. Ensemble learning models, particularly Random Forest classifiers, have demonstrated superior accuracy due to their ability to handle complex feature relationships. Recent research had also explored hybrid AI techniques combining ML and deep learning for improved performance.

EXISTING SYSTEM

Existing phishing detection system primarily depend on blacklist databases, signature-based detection, or manually designed heuristic rules. While these methods successfully identify previously known phishing websites, they struggle to detect newly created malicious URLs that have not yet been reported. Many browser-based security solutions require continuous database updates, increasing maintenance requirements. Traditional machine learning models often rely on complex feature engineering and may not provide real-time predictions. Furthermore, some detection systems exhibit lower accuracy due to insufficient feature selection or outdated datasets. These limitations reduce their effectiveness in preventing modern phishing attacks.

PROPOSED SYSTEM

The proposed Real-Time AI/ML Based Phishing Detection and Prevention System introduces an intelligent machine learning framework for detecting malicious URLs instantly. The system extracts multiple URL-based features such as URL length, subdomain count, digit frequency, HTTPS availability, special character usage, IP address presence, and suspicious symbols. These extracted features are provided to a Random Forest classifier trained on a large phishing dataset. The prediction result is immediately displayed through a Flask-based web application that classifies URLs as either legitimate or phishing. The proposed solution offers improved

detection accuracy, reduced false positives, faster prediction speed, and an easy-to-use interface suitable for cybersecurity applications.

SYSTEM ARCHITECTURE

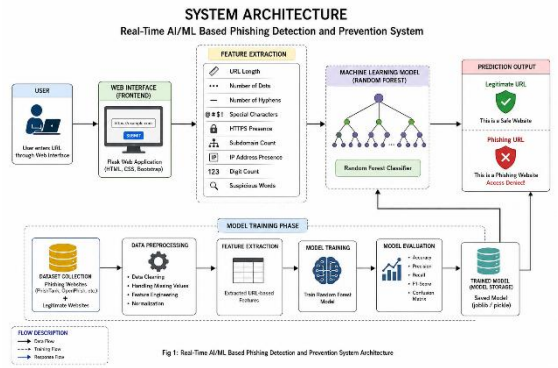


Fig 1: Real-Time AI/ML Based Phishing detection and Prevention System Architecture

METHODOLOGY DESCRIPTION

The methodology begins with collecting a labelled phishing URL dataset containing both legitimate and malicious website links. During preprocessing, unnecessary values are removed, and relevant URL-based features are extracted, including URL length, number of dots, hyphens, special characters, HTTPS usage, and numerical characters. These features are used to train a Random Forest classifier capable of distinguishing phishing websited from legitimate ones. The trained model is stored and integrated into a Flask web application. Whenever a user enters a URL, the system extracts the same features, performs prediction using the trained model, and immediately displays the classification result. Performance evaluation is conducted using accuracy, precision, recall, F1-score, and confusion matrix analysis to validate system effectiveness.

RESULTS AND DISCUSSION

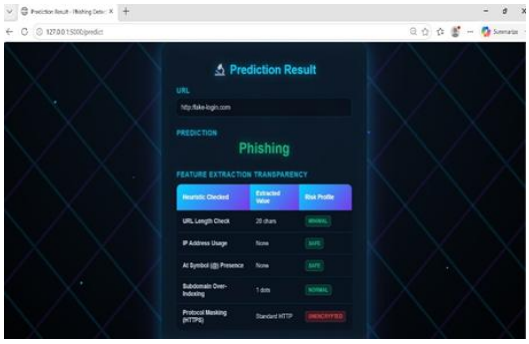


Fig 2: Real-Time URL prediction Output IS PHISHING

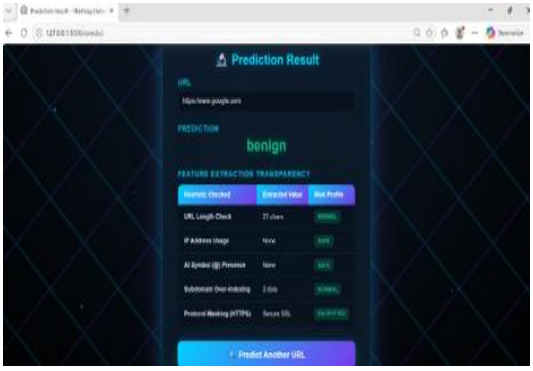


Fig 2: Real-Time URL prediction Output NORMAL

Experimental evaluation indicates that the proposed Random Forest model achieves high phishing detection accuracy while maintaining low prediction time. The system successfully identifies both legitimate and malicious URLs based on extracted URL feature. Real-time prediction enables users to receive immediate security alerts before accessing suspicious websites. Feature extraction significantly improves classification performance while reducing computational complexity. The Flask-based web interface provides an interactive environment for testing URLs, making the solution practical for educational and cybersecurity applications. Overall, the results confirm that AI/ML-based web interface provides an interactive environment for testing URLs, making the solution practical for educational and cybersecurity applications. Overall, the results confirm that AI/ML-based phishing detection offers reliable and

efficient protection against phishing attacks.

CONCLUSION

This research presents a real-time AI/ML Based Phishing Detection and Prevention System capable of accurately identifying phishing websites using machine learning techniques. The proposed Random Forest classifier effectively analyses URL features and provides instant predictions through a user-friendly web application. Compared with traditional blacklist-based approaches, the proposed system improves detection accuracy while supporting real-time analysis of newly generated phishing URLs. Experimental results demonstrate the reliability, efficiency, and scalability of the developed framework. The proposed solution contributes to enhancing cybersecurity awareness and reducing the risks associated with phishing attacks.

FUTURE SCOPE

Future enhancements may include integrating deep learning algorithms for improved phishing detection accuracy. Browser extensions can be developed to automatically analyze websites while users browse the internet. The system may also incorporate email phishing detection, webpage content analysis, and QR code verification to provide comprehensive cybersecurity protection. Cloud-based deployment can improve scalability for enterprise applications. Real-time threat intelligence feeds and continuously updated datasets can further enhance detection performance against emerging phishing attacks. Additionally, explainable AI techniques can be integrated to provide users with setailed reasons for each prediction, increasing transparency and trust in the system.

REFERENCES

1. T. M. Mitchell, Machine Learning. New York, NY, USA: McGraw-Hill, 1997.
2. Goodfellow, Y. Bengio, and A. Courville, Deep Learning. Cambridge, MA, USA: MIT Press, 2016.
3. C. M. Bishop, Pattern Recognition and Machine Learning. New York, NY, USA: Springer, 2006.
4. F. Pedregosa et al., "Scikit-learn: Machine Learning in Python," Journal of Machine Learning Research, vol. 12, pp. 2825–2830, 2011.
5. J. H. Friedman, "Greedy Function Approximation: A Gradient Boosting Machine," Annals of Statistics, vol. 29, no. 5, pp. 1189–1232, 2001.
6. L. Breiman, "Random Forests," Machine Learning, vol. 45, no. 1, pp. 5–32, Oct. 2001.
7. R. Verma and K. Dyer, "On the Character of Phishing URLs: Accurate and Robust Statistical Learning Classifiers," in Proc. ACM CODASPY, 2015, pp. 111–122.
8. M. Sahingoz, E. Buber, O. Demir, and B. Diri, "Machine Learning Based Phishing Detection from URLs," Expert Systems with Applications, vol. 117, pp. 345–357, Mar. 2019.
9. Y. LeCun, Y. Bengio, and G. Hinton, "Deep Learning," Nature, vol. 521, no. 7553, pp. 436–444, May 2015.
10. Akinyelu and A. Adewumi, "Classification of Phishing Email Using Random Forest Machine Learning Technique," Journal of Applied Security Research, vol. 16, no. 3, pp. 420–437, 2021.
11. PhishTank, "PhishTank: A Collaborative Clearing House for Phishing Data," 2025. [Online]. Available: https://phishtank.org

12. OpenPhish, "OpenPhish Phishing Intelligence," 2025. [Online]. Available: https://openphish.com
13. Google Safe Browsing, "Safe Browsing API Documentation," Google, 2025. [Online]. Available: https://safebrowsing.google.com
14. J. Han, M. Kamber, and J. Pei, Data Mining: Concepts and Techniques, 3rd ed. Burlington, MA, USA: Morgan Kaufmann, 2012.
15. S. Raschka and V. Mirjalili, Python Machine Learning, 3rd ed. Birmingham, U.K.: Packt Publishing, 2019.