Phishing Website Detection using Machine Learning

Ravindra Patil, Ashwini Changede, Akash Patekar, Shubham Satre

Department of Computer Science,

Rajarshi Shahu Mahavidyalaya, Deolali Pravara, India.

akashpatekar009@gmail.com, shubhamsatre610@gmail.com

This paper proposes a machine learning–based system for detecting phishing websites by analyzing URL, domain, and content-based features. The system aims to identify fraudulent websites that attempt to deceive users into revealing sensitive information such as login credentials and financial details. By eliminating reliance on traditional blacklist-based methods, the proposed approach enables proactive detection of newly created phishing websites. Supervised machine learning algorithms are trained to classify websites as legitimate or phishing with high accuracy. The system improves detection efficiency, reduces false positives, and supports real-time implementation for enhanced cybersecurity. The proposed solution contributes to improved online safety, transparency, and protection against cyber threats in modern digital environments.

INTRODUCTION

Phishing is a rapidly growing cybercrime in which attackers create fraudulent websites that closely imitate legitimate and trusted platforms such as banking portals, e-commerce websites, and social media services. The primary objective of these fake websites is to deceive users into revealing sensitive information like usernames, passwords, credit card details, and personal data. With the increasing dependence on online services, phishing attacks have become more frequent, sophisticated, and damaging.

Traditional phishing detection mechanisms, such as blacklist-based and rule-based systems, are limited in their effectiveness. These methods are reactive in nature and fail to detect newly generated phishing websites, commonly known as zero-day attacks. To overcome these challenges, machine learning techniques provide a proactive approach by learning patterns from historical data and identifying suspicious websites based on multiple features. This research focuses on developing an efficient phishing website detection system using machine learning algorithms to enhance online security.

RELATED WORK

Several research studies have been conducted in the domain of phishing website detection. Early approaches relied on blacklist-based detection, where known phishing URLs were stored and blocked. Although effective for previously identified attacks, these systems failed to detect newly created phishing websites.

Later research introduced heuristic and rule-based techniques that analyzed URL structures and webpage characteristics. With advancements in data science, machine learning-based approaches gained popularity. Algorithms such as Logistic Regression, Decision Trees, Support Vector Machines, and Random Forests were applied to phishing datasets obtained from sources like PhishTank and the UCI Machine Learning Repository. Recent studies have explored deep learning, natural language processing, and visual similarity analysis; however, these approaches often require high computational resources. This research builds upon existing work by focusing on lightweight, feature-based machine learning models suitable for real-time detection.

PROPOSED DUAL-MODE FRAMEWORK

The proposed system follows a dual-mode framework that combines feature-based analysis with machine learning-based classification. The first mode focuses on extracting and analyzing URL, domain, and content-based features, while the second mode applies trained machine learning models to classify websites as phishing or legitimate.

This dual-mode approach ensures accurate detection by leveraging both structural website characteristics and data-driven learning. The framework is designed to be scalable, efficient, and suitable for real-time deployment in browsers or enterprise security systems.

Objectives

The main objectives of this research are:

- To study various phishing attack techniques and patterns
- To identify distinguishing features of phishing websites
- To design a machine learning-based phishing detection system
- To evaluate the performance of multiple classification algorithms
- To develop a real-time phishing website detection prototype
- To improve user awareness regarding phishing threats

Hypothesis of the Study

The study is based on the hypothesis that machine learning algorithms can accurately distinguish between phishing and legitimate websites by analyzing URL, domain, and content-based features. It is assumed that feature-based learning models can detect new and unseen phishing websites more effectively than traditional blacklist-based approaches.

Significance of the Study

This study is significant as it addresses one of the most critical cybersecurity challenges faced by internet users today. By adopting a proactive machine learning-based approach, the proposed system reduces dependency on manual blacklist updates and improves detection accuracy. The system can help prevent financial losses, identity theft, and data breaches, making it valuable for individuals, organizations, and security solution providers.

Literature Review

Recent literature highlights the effectiveness of machine learning techniques in phishing detection. Researchers have demonstrated that feature-based classifiers can achieve high accuracy when trained on large and diverse datasets. Ensemble methods such as Random Forest have shown better performance compared to single classifiers. Despite these advancements, challenges such as dataset imbalance, adversarial attacks, and real-time deployment continue to motivate further research. This study contributes by focusing on practical implementation and comparative analysis of multiple algorithms.

Adoption of Phishing Detection Systems Before Intelligent Cybersecurity

Before the adoption of intelligent and machine learning–based cybersecurity systems, phishing website detection was primarily handled using traditional and manual approaches. Early detection mechanisms relied heavily on blacklist-based systems, where known phishing URLs were stored and blocked. While these methods were effective in preventing access to previously identified phishing websites, they failed to detect newly created or modified phishing sites.

Rule-based and heuristic methods were also used to identify phishing websites by checking predefined patterns such as suspicious keywords, URL length, or the presence of IP addresses. However, these systems lacked adaptability and were unable to cope with the continuously evolving techniques used by attackers. Frequent manual updates were required to maintain accuracy, making these systems inefficient and time-consuming.

Traditional systems were reactive rather than proactive, meaning phishing websites could cause damage before being detected and added to blacklists. Additionally, these methods often generated high false-positive rates, incorrectly blocking legitimate websites and affecting user experience.

The limitations of conventional phishing detection techniques highlighted the need for intelligent, automated solutions. This led to the adoption of machine learning-based phishing detection systems, which can analyze large datasets, learn complex patterns, and identify phishing websites in real time. The transition from static detection mechanisms to intelligent machine learning approaches laid the foundation for modern, adaptive, and scalable cybersecurity systems.

Research Methodology

The research methodology follows an experimental approach involving data collection, feature extraction, model training, and evaluation. Phishing and legitimate website datasets were collected from publicly available sources. Relevant features were extracted and preprocessed before training machine learning models. Model performance was evaluated using standard metrics such as accuracy, precision, recall, and F1-score.

Research Design

The research design is modular and consists of distinct components for data processing, feature extraction, model training, and prediction. This design ensures flexibility, scalability, and ease of future enhancements without affecting the overall system performance.

Challenges

Several challenges were encountered during the study, including dataset imbalance, feature selection complexity, and evolving phishing techniques. Additionally, ensuring real-time detection while maintaining high accuracy posed a significant challenge.

Results and Discussion

The experimental results demonstrate that machine learning models can effectively detect phishing websites. Among the evaluated algorithms, ensemble methods achieved higher accuracy and better generalization. The results confirm that the proposed system outperforms traditional detection techniques.

System Efficiency and Resource Utilization

The system requires minimal computational resources and can operate efficiently in real-time environments. Automated detection reduces manual intervention and improves resource utilization compared to traditional security systems.

Future Scope and Limitations

Future enhancements include the integration of deep learning models, browser extensions, and phishing email detection. While the current system performs well, continuous model retraining is required to handle evolving phishing strategies.

Limitations of the Proposed System

The system’s performance depends on dataset quality and feature selection. Advanced zero-day phishing attacks may evade detection, and the system currently focuses only on web-based phishing.

LIMITATIONS OF THE STUDY

The study is limited to experimental evaluation and does not include large-scale real-world deployment. Environmental and user behavior factors were not extensively analyzed.

Opportunities

With the growth of digital platforms and online services, there is significant opportunity to integrate machine learning-based phishing detection into browsers, enterprise security tools, and mobile applications. The system can contribute to building safer digital ecosystems.

Conclusion

This research concludes that machine learning provides an effective and proactive solution for phishing website detection. By analyzing multiple website features, the proposed system successfully identifies phishing attempts and enhances cybersecurity. The study demonstrates the potential of machine learning models for real-time and scalable phishing detection solutions.

References

1. Mohammad, R., Thabtah, F., & McCluskey, L. (2015). Predicting phishing websites using classification mining techniques.

2. Jain, A., & Gupta, S. (2017). Machine learning based phishing detection techniques.

3. PhishTank Dataset – https://www.phishtank.com

4. UCI Machine Learning Repository – Phishing Websites Dataset

5. Scikit-learn Documentation – https://scikit-learn.org