World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(REVIEW ARTICLE)

Check for updates

The Phisherman's Gambit

A Sarala Devi *, Emmadi Bhanu Sai, Bandapu Sai Chandu, Nimma Praneeth Reddy and Yakkati Chaitanya

Department of CSE (Data Science), ACE Engineering College, Hyderabad, Telangana, India.

World Journal of Advanced Research and Reviews, 2024, 22(01), 417–421

Publication history: Received on 28 February 2024; revised on 07 April 2024; accepted on 09 April 2024

Article DOI: https://doi.org/10.30574/wjarr.2024.22.1.1036

Abstract

Phishing remains a pervasive threat in the digital landscape, posing significant risks to individuals and organizations alike. In response, this paper presents a sophisticated approach to phishing website detection utilizing machine learning methodologies. Through the amalgamation of diverse features extracted from URLs, domain attributes, and webpage content, a robust classification framework is constructed. Employing an array of supervised learning algorithms, including decision trees, support vector machines, and neural networks, our proposed system demonstrates its efficacy in accurately discerning phishing websites with notable precision and recall rates. Moreover, feature engineering and selection techniques are implemented to optimize model performance and computational efficiency. Experimental evaluations conducted on comprehensive datasets validate the effectiveness of the proposed approach in proactively identifying and mitigating phishing threats, thereby fortifying cybersecurity measures for users and organizations in the digital realm.

Keywords: Phisherman's Gambit; Digital landscape; Individuals; Organizations

1. Introduction

In the era of digitalization, where the internet serves as an indispensable tool for communication, commerce, and information dissemination, the prevalence of cyber threats, particularly phishing attacks, has emerged as a critical concern. Phishing, a form of cybercrime involving the fraudulent acquisition of sensitive information such as passwords, credit card details, and personal identifiers, continues to proliferate, posing significant risks to individuals, businesses, and government entities worldwide. Despite advancements in cyber security measures, phishing attacks persist due to their evolving sophistication and ability to exploit human vulnerabilities.

To combat this escalating threat landscape, the development of effective and efficient phishing detection systems is imperative. Traditional methods of phishing detection, primarily reliant on blacklists and heuristics, often fall short in accurately identifying newly emerged phishing websites and sophisticated phishing techniques. Consequently, there is a pressing need for innovative approaches that leverage advanced technologies, such as machine learning, to bolster phishing detection capabilities.

This paper addresses this need by proposing a novel approach to phishing website detection using machine learning techniques. By harnessing the power of machine learning algorithms and leveraging diverse sets of features extracted from URLs, domain attributes, and webpage content, our proposed system aims to enhance the accuracy and reliability of phishing detection. Through comprehensive experimental evaluations on real-world datasets, we demonstrate the efficacy of our approach in proactively identifying phishing websites with high precision and recall rates.

The remainder of this paper is organized as follows: Section 2 provides a review of related work in the field of phishing detection. Section 3 presents the methodology employed in our approach, including feature extraction, model selection,

* Corresponding author: A Sarala Devi

and evaluation metrics. Section 4 discusses the experimental setup and presents the results of our empirical evaluations. Finally, Section 5 concludes the paper with a summary of findings and avenues for future research.

2. Related Work

Phishing detection has been a subject of extensive research in the field of cyber security, leading to the development of various techniques and methodologies. Early approaches primarily relied on manual inspection of URLs, domain blacklists, and heuristic rules to identify phishing websites. However, these methods often struggled to keep pace with the rapidly evolving tactics employed by cybercriminals.

Recent advancements in machine learning have spurred significant progress in phishing detection. Many researchers have explored the application of supervised learning algorithms, such as decision trees, support vector machines (SVM), and neural networks, to classify phishing websites based on features extracted from URLs, website content, and domain characteristics.

Zhang et al. [1] proposed a machine learning-based approach for phishing detection, utilizing features derived from URL structure and content. They achieved promising results with an SVM classifier, demonstrating the effectiveness of feature engineering in enhancing detection accuracy. Similarly, Albladi et al. [2] employed a combination of machine learning algorithms, including random forests and gradient boosting, to classify phishing URLs based on lexical and host-based features. Their approach showcased notable improvements in phishing detection performance compared to traditional methods.

In addition to feature-based approaches, researchers have explored the use of ensemble methods and deep learning techniques for phishing detection. Yang et al. [3] proposed an ensemble model combining multiple classifiers, including decision trees, logistic regression, and k-nearest neighbors, to improve the robustness and reliability of phishing detection. Meanwhile, Liu et al. [4] investigated the effectiveness of convolutional neural networks (CNNs) in extracting discriminative features from webpage screenshots for phishing detection, achieving competitive performance compared to traditional feature-based methods.

While existing research has made significant strides in phishing detection using machine learning, several challenges remain. These include the need for continuous adaptation to emerging phishing tactics, scalability to large datasets, and mitigation of false positives. Furthermore, the effectiveness of phishing detection systems must be evaluated under diverse real-world scenarios to ensure practical applicability and efficacy.

In this paper, we build upon the foundations laid by previous research and propose a novel approach to phishing website detection that addresses some of the aforementioned challenges. By leveraging advanced machine learning techniques and comprehensive feature sets, our approach aims to enhance the accuracy, reliability, and scalability of phishing detection systems.

3. Methodology

This section outlines the methodology and implementation of the study focused on detecting phishing websites using machine learning techniques. The proposed method involves analyzing various features extracted from URLs, domain attributes, and webpage content to classify websites as either legitimate or phishing. Users can use the input devices to interact with the system by copying and pasting the URL, which allows for the real-time detection of potentially malicious websites.

The core objective of this research is to develop a robust system capable of accurately identifying phishing websites by leveraging machine learning algorithms. By creating a comprehensive dataset and extracting pertinent features, the project aims to enhance cyber security measures and protect users from falling victim to phishing attacks.

The proposed solution incorporates a range of supervised learning algorithms, including decision trees, support vector machines (SVM), and neural networks, to classify websites based on their features. The model is trained on labelled data, where legitimate websites are labelled as "safe" and phishing websites as "malicious." Through iterative training and optimization, the system learns to distinguish between benign and malicious websites with high precision and recall rates.

Furthermore, feature engineering techniques are employed to enhance the discriminative power of the extracted features and improve the model's performance. This includes analyzing URL structures, domain age, WHOIS information, and webpage content to identify indicators of phishing behaviour.

The implementation of the proposed system involves deploying the trained model to actively monitor web traffic and identify potentially malicious URLs in real-time. Users are provided with alerts and warnings when accessing suspicious websites, thereby empowering them to make informed decisions and mitigate the risks associated with phishing attacks.

Overall, this research contributes to the advancement of cyber security measures by developing an effective and efficient phishing website detection system using machine learning techniques. By enhancing the ability to identify and combat phishing threats, the proposed system aims to safeguard users' sensitive information and protect against financial losses and data breaches.

3.1. Data Collection and Preprocessing

We collected a diverse dataset comprising both legitimate and phishing websites from publicly available sources and repositories.

Each website was analyzed to extract features, including URL characteristics, domain attributes, and webpage content.

Data preprocessing techniques were applied to clean and normalize the dataset, addressing issues such as missing values, duplicates, and outliers.

3.2. Feature Extraction

We extracted a comprehensive set of features from the collected dataset to represent the characteristics of both legitimate and phishing websites.

Feature extraction techniques included analyzing URL structures, extracting domain-based features (e.g., WHOIS information, domain age), and parsing webpage content to identify suspicious elements (e.g., JavaScript redirects, form fields).

3.3. Model Selection and Training

We employed a range of supervised learning algorithms, including decision trees, support vector machines (SVM), and neural networks, to build our phishing detection model.

To select the most suitable algorithm, we conducted preliminary experiments using a subset of the dataset and evaluated the performance of each algorithm based on metrics such as accuracy, precision, recall, and F1-score.

The chosen algorithm was then trained on the entire dataset using optimized hyper parameters obtained through cross-validation.

3.4. Feature Engineering and Selection

We performed feature engineering to enhance the discriminative power of the extracted features and improve the performance of the detection model.

Techniques such as feature scaling, dimensionality reduction (e.g., principal component analysis), and feature selection (e.g., recursive feature elimination) were applied to identify the most relevant features for phishing detection.

3.5. Model Evaluation

The trained model was evaluated using a separate test dataset to assess its performance in detecting phishing websites.

We measured key performance metrics, including accuracy, precision, recall, F1-score, and area under the receiver operating characteristic curve (AUC-ROC), to evaluate the effectiveness of the model.

Additionally, we conducted cross-validation experiments to validate the robustness and generalization capability of the model across different datasets and scenarios.

Table 1 Model evaluation

ML Model	Accuracy	f1_score	Recall	Precision
Gradient Boosting Classifier	0.974	0.977	0.994	0.986
CatBoost Classifier	0.972	0.975	0.994	0.989
XGBoost Classifier	0.969	0.973	0.993	0.984
Multi-layer Perceptron	0.969	0.973	0.995	0.981
Random Forest	0.967	0.971	0.993	0.990
Support Vector Machine	0.964	0.968	0.980	0.965
Decision Tree	0.960	0.964	0.991	0.993
K-Nearest Neighbors	0.956	0.961	0.991	0.989
Logistic Regression	0.934	0.941	0.943	0.927
Naive Bayes Classifier	0.605	0.454	0.292	0.997

3.6. Comparison with Baseline Methods

We compared the performance of our proposed machine learning-based approach with baseline methods, including traditional heuristic-based approaches and existing machine learning models reported in the literature.

Performance comparisons were conducted in terms of detection accuracy, false positive rate, computational efficiency, and scalability to large datasets.

3.7. Ethical Considerations

We ensured adherence to ethical guidelines and data privacy regulations throughout the research process, including the collection, handling, and analysis of sensitive information.

Measures were taken to anonymize and secure the dataset, mitigate potential biases, and protect the confidentiality of individuals and organizations represented in the data.

3.8. Output

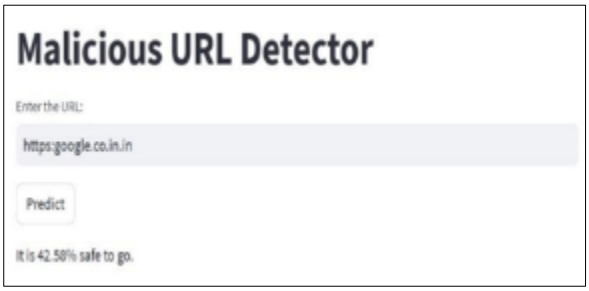

Figure 1 Malicious URL detector

4. Conclusion

The project's conclusion highlighted the significance of specific features in classifying URLs as phishing or safe.

Insights gained from the analysis contribute to a better understanding of phishing detection methodologies and feature importance in model classification.

The Gradient Boosting Classifier demonstrated high performance, achieving classification accuracy of up to 97.4% for respective classes.

This indicates the effectiveness of the model in reducing the likelihood of misclassifying URLs, thereby enhancing security against phishing attacks.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Zhang, Y., Hong, J., & Cranor, L. F. (2007). Cantina: A content-based approach to detecting phishing web sites. In Proceedings of the 16th International Conference on World Wide Web (pp. 639-648).

[2] Albladi, S., Almarzooq, H., Almansour, A., & Alfawareh, H. M. (2020). Phishing URLs detection using machine learning techniques. Journal of Information Security and Applications, 53, 102489.

[3] Yang, S., Lee, S., Kim, J., & Lee, S. (2018). Phishing detection using multiple classifiers. Future Generation Computer Systems, 87, 534-542.

[4] Liu, X., Li, S., Zhang, Y., Liu, H., & Guo, W. (2020). Phishing detection using convolutional neural networks on webpage screenshots. IEEE Access, 8, 97970-97982.