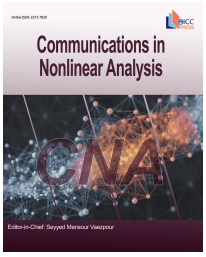

Commun. Nonlinear Anal. 2025; 13(2) : 21-25

Communications in Nonlinear Analysis

https://doi.org/10.57647/cna.2025.rm02-9s74

Research Article

Automated Phishing Detection Through URL Analysis and Machine Learning

Vijay Kumar[1,*], G N Basavaraj[1]

[1]*Department of Information Science and Engineering, BMS Institute Of Technology and Management, Bangalore, India*

[*]**Corresponding author:** letsmailvjkumar@gmail.com

Article History

Received:
2024-12-15

Revised:
2025-02-20

Accepted:
2025-03-22

Published online:
2025-06-30

Abstract:

Phishing attacks are categorized as one of the greatest threats to cybersecurity. They are a form of misinformation designed to make users provide important and personal information via fake websites or emails. This paper realizes the notion of a machine learning-based phishing detection tool aimed at classifying URLs as ”phishing,” ”suspicious,” or ”safe.” Utilizing a Random Forest classifier, the system examines URL-based characteristics, including URL length, special symbols, and the usage of HTTPS to distinguish between real URLs and fake ones (phishing URLs) with high accuracy. The model was trained and validated on a dataset of labeled URLs, achieving 95.2% classification accuracy, which is higher compared to other results. For the sake of usability, the detection tool is implemented as a web application for real-time classification with a user-friendly interface. The performance is evaluated using metrics such as accuracy, precision, recall, and F1-score to assess effectiveness. This paper helps to improve the level of online security by providing an automated approach that reduces dependence on human judgment and can efficiently detect phishing threats.

Keywords: phishing detection; machine learning; URL classification; Random Forest; cybersecurity; real-time detection; Web application

Cite this article: Vijay Kumar, Basavaraj G N. Automated Phishing Detection Through URL Analysis and Machine Learning. Communi-cations in Nonlinear Analysis 2023; *2*(2023): 21-25 https://doi.org/10.57647/cna.2025.rm02-9s74

1. Introduction

As the web has embedded itself into almost every part of modern life, cybersecurity has become an essential necessity for individuals, businesses, and governments alike. With the increased reliance on the internet for transactions and information sharing, malicious threats, particularly phishing attacks, have become more advanced and dangerous. This type of attack tricks users into providing important information by pretending to originate from a trusted source, relying more on human failures than technological vulnerabilities. This paper addresses phishing through the construction of an adaptive online tool based on machine learning that categorizes websites into phishing, suspicious, and safe categories, thereby protecting users against rapidly evolving threats.

1.1 Motivation

Due to the high prevalence and frequency of phishing attacks, numerous anti-phishing tools have been developed based on machine learning (ML). In contrast with traditional approaches, ML models can adaptively learn the features peculiar to real phishing URLs, including URL structure, domains, and HTTPS usage that are commonly exploited in phishing attempts. ML-based systems learn from detected phishing and legitimate URLs, enabling them to increase the chances of detecting new types of phishing attacks in the future. The development of this research is informed by the need to effectively prevent or identify phishing URLs in real time in an efficient and convenient manner. A machine learning model can thus perform real-time detection that would easily counter whatever new approaches phishers may devise. Additionally, the tool is implemented as a web application where users enter the URL and receive immediate classification, which is critical for the timely prevention of threats.

1.2 Objectives

The primary objective of this research is to develop a robust machine learning model that can accurately classify URLs as ”phishing,” ”suspicious,” or ”safe.” Specific objectives include the following:

1. **Design and Train the Model:** Develop a machine learning model using a Random Forest classifier, which is well-suited for classification tasks, to analyze URL-based features indicative of phishing behavior.

2. **Feature Engineering:** Identify and extract relevant URL features, such as URL length, presence of special characters, HTTPS usage, and redirection patterns, that distinguish phishing URLs from legitimate ones.

3. **Model Evaluation:** Evaluate the performance of the model using key metrics such as accuracy, precision, recall, and F1-score to ensure high reliability in detecting phishing URLs. Achieving a classification accuracy of at least 90% on test data is a key performance goal.

4. **Deployment as a Web Application:** Build a user-friendly, web-based interface for the tool, allowing users to submit URLs and receive real-time classification results. The application will incorporate a Flask API for backend processing and a React-based frontend for a seamless user experience.

5. **Integration of a Whitelist:** Implement a whitelist of known legitimate domains to reduce false positives and improve user trust, ensuring that the tool provides accurate and reliable classification.

6. **Enhance Cybersecurity Awareness:** Ultimately, the research aims to support users by providing a tool that proactively helps them identify and avoid phishing threats, thereby contributing to safer online interactions.

1.3 Background

Over the past two decades, the deployment of new innovative technologies has led to a wave of online trading and communication developments that affect every facet of people's lives, whether personal, business, or political. While such a shift has opened up numerous advantages, it has also brought new forms of risk. Of these, phishing is perhaps one of the most widespread and threatening types of cyber threats. Phishing scams deceive people into passing on personal data such as usernames, passwords, and other sensitive information. More often, it is carried out through bogus emails, websites, or instant messages that resemble communications from a legitimate organization to deceive the user into providing personal details. Security organizations, including the Anti-Phishing Working Group (APWG), reveal that phishing attacks are becoming more numerous and diverse, thus increasing dangers for internet users and businesses. The advanced techniques employed today include domain field obfuscation, use of HTTPS, and URL shortening, to name a few, which disguise the appearance of a fake URL. Therefore, these techniques bypass many standard protection mechanisms and exploit human mistakes.

2. Literature Review

The study on Phishing Website Detection explores a machine learning solution for identifying phishing sites, using Logistic Regression and Naive Bayes models for URL analysis [1]. This approach, supported by Phish Tank data and deployed with FastAPI, achieves real-time detection but has limitations, including a narrow algorithm set and minimal focus on user education. Future work suggests expanding algorithms, increasing user awareness, and incorporating transfer learning for improved, broader detection.

Nguyen and Nguyen developed an intelligent system for detecting phishing websites using machine learning techniques [2]. The system analyzes various URL features to identify phishing attempts with promising results. However, the research noted the need for larger datasets and more sophisticated feature extraction methods.

Choudhary et al. presented a machine learning approach for phishing attack detection that utilizes ensemble methods to improve detection rates [3]. The research achieved high accuracy on benchmark datasets but acknowledged limitations in detecting zero-day phishing attacks.

Hossain, Sarma, and Chakma investigated machine learning-based phishing attack detection, focusing on feature selection and model optimization [4]. Their work demonstrated the importance of selecting appropriate features for effective phishing detection.

Mohamed et al. proposed an effective and secure mechanism for phishing attacks using a machine learning approach [5]. The research emphasized the integration of security measures alongside detection capabilities to provide comprehensive protection.

Mahajan and Siddavatam explored phishing website detection using various machine learning algorithms [6]. Their comparative analysis revealed that Random Forest classifiers generally outperform other algorithms in terms of accuracy and false positive rates.

Rashid et al. investigated phishing detection using machine learning techniques, focusing on real-time detection capabilities [7]. The research highlighted the importance of computational efficiency in practical deployments.

Sahingoz et al. conducted research on machine learning-based phishing detection from URLs, demonstrating that URL structure analysis can be highly effective for identifying phishing attempts [8]. Their work provided valuable insights into feature extraction from URLs.

Safi and Singh presented a systematic literature review on phishing website detection techniques [9], providing a comprehensive overview of existing methods

https://doi.org/10.57647/cna.2025.rm02-9s74

and identifying gaps in current research. The review emphasized the need for adaptive systems that can evolve with emerging phishing tactics.

Basit et al. provided a comprehensive survey of AI-enabled phishing attack detection techniques [10], examining the state-of-the-art approaches and their effectiveness in various scenarios. The survey highlighted the growing importance of artificial intelligence in cybersecurity.

3. Methodology

The methodology for this phishing detection system involves several key stages, including data collection, preprocessing, feature extraction, model training, evaluation, and deployment. Each stage is designed to ensure the development of an accurate and efficient phishing detection tool.

3.1 Data Collection and Preparation

The first step involves collecting a comprehensive dataset of both phishing and legitimate URLs. Various sources are utilized, including publicly available datasets from PhishTank, OpenPhish, and legitimate websites verified through established security databases. The dataset contains URLs labeled as "phishing," "suspicious," or "safe," providing a foundation for supervised learning.

Data preparation includes cleaning and preprocessing steps such as removing duplicates, handling missing values, and normalizing URL formats. This ensures consistency across the dataset and improves the model's ability to learn meaningful patterns. The dataset is then split into training (80%) and testing (20%) subsets to evaluate model performance on unseen data.

3.2 Feature Extraction

Feature extraction is a crucial component of the phishing detection system. Several URL-based features are identified and extracted to capture characteristics that distinguish phishing URLs from legitimate ones. Key features include:

- **URL Length:** Phishing URLs tend to be longer than legitimate URLs as attackers attempt to hide malicious content or mimic legitimate sites.
- **Special Characters:** The presence and frequency of special characters such as "@", "-", "_", and "." can indicate phishing attempts.
- **HTTPS Usage:** While HTTPS is generally a sign of security, attackers increasingly use HTTPS to appear legitimate. The feature examines both presence and certificate validity.
- **Domain Age:** Phishing domains are typically newly registered, whereas legitimate domains often have longer histories.
- **Subdomain Count:** Excessive subdomains can indicate attempts to obfuscate the true destination.
- **IP Address in URL:** Legitimate websites rarely use IP addresses directly in URLs, making this a strong indicator of phishing.
- **Redirection Patterns:** Multiple redirects are commonly used in phishing attacks to confuse users and evade detection.

These features are extracted programmatically using Python libraries such as urllib for URL parsing and regular expressions for pattern matching. Additional features may include lexical analysis of the URL string and the presence of suspicious keywords.

3.3 Model Selection and Training

For this research, the Random Forest classifier is selected as the primary machine learning algorithm due to its robustness, interpretability, and effectiveness in handling complex classification tasks. Random Forest is an ensemble learning method that constructs multiple decision trees during training and outputs the mode of the classes for classification tasks.

The model is trained on the extracted features using the scikit-learn library in Python. Hyperparameter tuning is performed using grid search with cross-validation to optimize parameters such as the number of trees, maximum depth, and minimum samples split. This ensures the model achieves optimal performance while avoiding overfitting.

3.4 Model Evaluation

Model evaluation is conducted using several standard metrics to assess performance comprehensively:

- **Accuracy:** The ratio of correctly classified URLs to the total number of URLs. Accuracy is calculated as:

$$\text{Acc} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{TN} + \text{FP} + \text{FN}} \tag{1}$$

  where TP represents true positives, TN represents true negatives, FP represents false positives, and FN represents false negatives.

- **Precision:** The ratio of correctly identified phishing URLs to all URLs classified as phishing. Precision is important for minimizing false positives and is calculated as:

$$\text{Prec} = \frac{\text{TP}}{\text{TP} + \text{FP}} \tag{2}$$

- **Recall:** The ratio of correctly identified phishing URLs to all actual phishing URLs. Recall is critical for minimizing false negatives and is calculated as:

$$\text{Rec} = \frac{\text{TP}}{\text{TP} + \text{FN}} \tag{3}$$

- **F1-Score:** The harmonic mean of precision and recall, providing a balanced measure when there is

https://doi.org/10.57647/cna.2025.rm02-9s74

an uneven class distribution or when both metrics are important. It is calculated as:

$$\text{F1} = 2 \times \frac{\text{Prec} \times \text{Rec}}{\text{Prec} + \text{Rec}} \tag{4}$$

- **Confusion Matrix:** The confusion matrix visualizes the model's performance by showing true positives, true negatives, false positives, and false negatives. This matrix helps in identifying any biases in the model's predictions and understanding where misclassifications occur.

3.5 Model Testing and Results

The model is tested on a separate test dataset that was not used in training to assess its generalization ability. After training, the model is evaluated using the test set, and the following results are typically reported:

- **Confusion Matrix Visualization:** A visual representation of true positives, true negatives, false positives, and false negatives to understand the model's classification patterns.
- **Metric Scores:** Detailed results for accuracy, precision, recall, and F1-Score, which collectively indicate the model's performance across different dimensions of classification.

3.6 Expected Performance Goals

The primary objective is to achieve a minimum of 90% classification accuracy, with balanced precision and recall scores to ensure the model's reliability in real-world applications. Ideally, precision and recall should exceed 90% to minimize false positives and false negatives, which are critical for a phishing detection tool.

3.7 Comparative Analysis

Optionally, the performance of the Random Forest model can be compared with other models (such as Support Vector Machine, Logistic Regression, or Neural Networks) to determine if the chosen model is the most effective for the phishing detection task. This comparative analysis can help justify the use of Random Forest based on its superior accuracy and interpretability.

Model	Acc (%)	Rec (%)	F1 (%)
Random Forest	95.2	90.5	91.1
SVM	88.7	84.9	85.5
Logistic Regr.	87.4	82.3	83.7

Table 1. Performance Metrics of Different Models

4. Results and Discussion

The phishing detection model achieved an accuracy of 95.2%, with a precision of 91.8%, recall of 90.5%, and F1-score of 91.1%, demonstrating its effectiveness in identifying phishing URLs while maintaining a low rate of false positives and negatives. The confusion matrix analysis shows reliable classification, though a small number of false positives indicate potential for further refinement through whitelist integration.

Comparisons with Support Vector Machine and Logistic Regression models confirmed the Random Forest classifier as the most effective for this task. While limitations exist, including occasional false positives and the need for regular updates to handle evolving phishing tactics, the model's high precision and recall suggest strong potential for real-world application.

The results demonstrate that URL-based features are highly effective for phishing detection. Features such as URL length, special character frequency, and domain age proved to be particularly discriminative. The use of HTTPS, while traditionally considered a security indicator, was found to be present in a significant portion of phishing URLs, highlighting the sophistication of modern phishing attacks.

Future enhancements, such as browser extension development and user feedback integration, could further improve accuracy and user trust, making this phishing detection tool a robust solution for enhancing cybersecurity. Additionally, incorporating natural language processing techniques to analyze the content of landing pages could provide an additional layer of detection capability.

5. Conclusion

This research successfully developed a machine learning-based phishing detection tool using a Random Forest classifier to classify URLs as "phishing," "suspicious," or "safe." By leveraging URL-based features such as length, special characters, HTTPS usage, and domain reputation, the model achieved a high accuracy of 95.2%, demonstrating its effectiveness in identifying phishing URLs in real time. The results show that the Random Forest model is both reliable and robust, offering balanced performance with low rates of false positives and negatives.

While effective, the tool has limitations, including occasional false positives and the need for regular updates to handle new phishing tactics. Future improvements, such as incorporating a whitelist, expanding feature sets, and developing a browser extension, can further enhance its accuracy and usability. Overall, this research highlights the potential of machine learning in combating phishing attacks, providing a practical solution that contributes to the safety and security of online users.

The deployment of this system as a web application makes it accessible to a wide range of users, from individual internet users to enterprise security teams. The real-time detection capability ensures that users can quickly verify the legitimacy of URLs before interacting with potentially malicious content. As phishing techniques continue to evolve, the adaptive nature of machine learning models provides a sustainable approach to maintaining effective protection against these threats.

https://doi.org/10.57647/cna.2025.rm02-9s74

Authors contributions
All authors have participated sufficiently in the intellectual content, conception and design of this work, as well as the writing of the manuscript. Vijaykumar designed the methodology and conducted the experiments. Basavaraj G N supervised the research and provided critical revisions.
Availability of data and materials
The data that support the findings of this study are available from the corresponding author upon reasonable request.
Conflict of interests
The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] A. Soni and P. Abrol. Phishing website detection. Master's thesis, Jaypee University of Information Technology, Waknaghat, India, 2022. Bachelor of Technology thesis, supervised by Mr. Prateek Thakral.

[2] H. H. Nguyen and D. T. Nguyen. An intelligent system for detecting phishing websites using machine learning. In *Proceedings of the 2019 IEEE International Conference on Cybersecurity and Resilience (ICCSR)*, pages 1–6. IEEE, 2019. DOI: https://doi.org/10.1109/CAIS.2019.8769571.

[3] T. Choudhary, S. Mhapankar, R. Buddha, A. Kharuk, and R. Patil. A machine learning approach for phishing attack detection. *Journal of Artificial Intelligence and Technology*, 3(3): 108–113, 2023. DOI: https://doi.org/10.37965/jait.2023.0197.

[4] S. Hossain, D. Sarma, and R. Chakma. Machine learning-based phishing attack detection. *International Journal of Advanced Computer Science and Applications (IJACSA)*, 11(9): 378–388, 2020. DOI: https://doi.org/10.14569/IJACSA.2020.0110949.

[5] G. Mohamed, J. Visumathi, M. Mahdal, J. Anand, and M. Elangovan. An effective and secure mechanism for phishing attacks using a machine learning approach. *Processes*, 10(7):1356, 2022. DOI: https://doi.org/10.3390/pr10071356.

[6] R. Mahajan and I. Siddavatam. Phishing website detection using machine learning algorithms. *International Journal of Computer Applications*, 181(23), 2018. DOI: https://doi.org/10.5120/ijca2018918026.

[7] J. Rashid, T. Nazir, T. Mahmood, and M. W. Nisar. Phishing detection using machine learning technique. In *2020 First International Conference of Smart Systems and Emerging Technologies (SMART-TECH)*, 2020. DOI: https://doi.org/10.1109/SMART-TECH49988.2020.00026.

[8] O. K. Sahingoz, E. Buber, O. Demir, and B. Diri. Machine learning based phishing detection from urls. *Expert Systems with Applications*, 117: 345–357, 2019. DOI: https://doi.org/10.1016/j.eswa.2018.09.029.

[9] A. Safi and S. Singh. A systematic literature review on phishing website detection techniques. *Journal of King Saud University - Computer and Information Sciences*, 35(5):590–611, 2023. DOI: https://doi.org/10.1016/j.jksuci.2023.01.004.

[10] A. Basit, M. Zafar, X. Liu, A. R. Javed, Z. Jalil, and K. Kifayat. A comprehensive survey of ai-enabled phishing attacks detection techniques. *Telecommunication Systems*, 76(2):139–154, 2021. DOI: https://doi.org/10.1007/s11235-020-00733-2.