IJARSCT

International Journal of Advanced Research in Science, Communication and Technology

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

ISSN: 2581-9429

Volume 5, Issue 3, June 2025

Impact Factor: 7.67

Detecting Phishing Attacks Using Machine Learning Algorithms: SVM, Naive Bayes, and Random Forest

Prof. Mrs. R. A. Patil , Bharti Onkar, Mekhle Anshul, Mengawade Darshan, Patil Rugved

Smt. Kashibai Navale College of Engineering, Pune, Maharashtra, India

Abstract: *Phishing attacks have emerged as a prevalent and serious cyber threat, taking advantage of human weaknesses to obtain sensitive information like passwords and financial details. Early detection of phishing attempts can help avert serious repercussions, including identity theft and financial loss. Machine learning (ML) techniques have demonstrated considerable potential in automating the identification of phishing websites, utilizing data-driven insights to categorize URLs or website characteristics as either malicious or safe. This paper assesses the performance of three widely used machine learning algorithms for phishing detection: Support Vector Machine (SVM), Naive Bayes (NB), and Random Forest (RF). We offer a thorough comparison of these algorithms based on their accuracy, precision, recall, and F1-score, utilizing a publicly available phishing dataset..*

Keywords: Phishing attacks

I. INTRODUCTION

Phishing attacks involve cybercriminals trying to trick users into revealing sensitive information by masquerading as a legitimate entity. These attacks are usually carried out through emails or counterfeit websites that mimic authentic online platforms. According to the Anti-Phishing Working Group (APWG), phishing attacks have been on the rise, resulting in millions of dollars lost each year due to these schemes. With the vast number of phishing websites currently active, it has become crucial to create automated systems that can detect phishing attempts and safeguard users. Machine learning (ML) techniques are increasingly being utilized in cybersecurity to identify phishing websites, offering a more dependable and scalable solution compared to traditional rule-based approaches. In this paper, we delve into the use of three well-known ML algorithms—Support Vector Machine (SVM), Naive Bayes (NB), and Random Forest (RF)—for detecting phishing websites.

II. LITERATURE REVIEW

Previous research on phishing detection has explored a range of methods, including heuristic-based techniques, rule-based systems, and machine learning algorithms. Some of the most frequently utilized ML techniques are:

- **Support Vector Machine (SVM):** SVM is widely recognized for its effectiveness in classification tasks within cybersecurity, as it identifies optimal hyperplanes that maximize the margin between different classes. Its robustness in high-dimensional spaces makes it particularly suitable for detecting phishing websites by analyzing features like URL length, domain details, and the presence of special characters.
- **Naive Bayes (NB):** Naive Bayes is a probabilistic classifier grounded in Bayes' theorem. It operates under the assumption that features are independent, which can be advantageous in phishing detection, especially when the dataset includes features that independently influence the classification, such as domain age and URL attributes.
- **Random Forest (RF):** Random Forest is an ensemble learning technique that aggregates the predictions from multiple decision trees. It is well-regarded for its capacity to manage large datasets and uncover complex relationships among features, making it a strong option for phishing detection.

DOI: 10.48175/IJARSCT-27577

Numerous studies have reported encouraging outcomes with these algorithms. For instance, SVM has demonstrated high accuracy in identifying phishing websites, while Random Forest is noted for its stability and robustness. Naive Bayes is valued for its simplicity and efficiency, especially in real-time scenarios where speed is essential.

III. METHODOLOGY

3.1 Dataset

In this study, we utilized the Phishing Website Dataset from the UCI Machine Learning Repository. This dataset comprises 30 features, which include both URL-based and domain-based attributes, such as the length of the URL, the number of dots present in the URL, whether the domain is newly registered, and the occurrence of suspicious words within the URL.

The dataset is categorized into two groups: phishing (malicious) and legitimate (non-malicious) websites. It is further divided into 70% for training and 30% for testing.

3.2 Preprocessing

To prepare the dataset for machine learning algorithms, several preprocessing steps were undertaken:

- **Normalization:** All numeric features were scaled to a range of [0, 1] to ensure that features with larger numerical values do not dominate the learning process.
- **Handling Missing Values:** Missing values were addressed by imputing the mean for continuous features and the mode for categorical features.
- **Feature Selection:** The feature set was refined through correlation analysis to remove redundant features, enhancing model efficiency and minimizing overfitting.

3.3 Algorithms

The following three algorithms were employed for detecting phishing websites:

1. **Support Vector Machine (SVM):** We implemented a radial basis function (RBF) kernel for SVM, which is recognized for its effectiveness in non-linear classification tasks. Hyperparameters, including the penalty parameter (C) and the kernel coefficient (gamma), were optimized using grid search with cross-validation.
2. **Naive Bayes (NB):** The Naive Bayes classifier was applied to the dataset, utilizing the Gaussian Naive Bayes implementation, which presumes that the features adhere to a Gaussian distribution. The model's performance was assessed without additional parameter tuning, as Naive Bayes is generally robust to hyperparameter variations.
3. **Random Forest (RF):** Random Forest was employed with 100 trees, a common choice that strikes a balance between model complexity and computational efficiency. Hyperparameters such as tree depth and the number of features considered were also adjusted.

IV. RESULTS AND DISCUSSION

4.1 Performance Comparison

The results of the experiments are presented in Table 1, which summarizes the performance metrics for SVM, Naive Bayes, and Random Forest on the phishing dataset.

Algorithm	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
Support Vector Machine (SVM)	**97.5**	**98.3**	**96.2**	**97.2**
Naive Bayes (NB)	**93.4**	**94.1**	**92.5**	**93.3**
Random Forest (RF)	**96.9**	**97.4**	**95.6**	**96.5**

DOI: 10.48175/IJARSCT-27577

- **SVM:** The Support Vector Machine demonstrated the highest accuracy, precision, and F1-score, establishing it as the most effective algorithm in this study. Its capability to identify a clear decision boundary in high-dimensional space played a key role in its outstanding performance in detecting phishing websites.
- **Naive Bayes**: Although Naive Bayes exhibited the lowest performance compared to SVM and Random Forest, it still achieved a commendable accuracy of 93.4%. Its simplicity and speed make it a viable option for real-time applications where computational efficiency is crucial.
- **Random Forest:** Random Forest showed strong performance with an accuracy of 96.9%. Its ability to manage feature interactions and noise made it a competitive choice, even though it was slightly less accurate than SVM. Nonetheless, it offered a good balance between accuracy and interpretability.

4.2 Implications for Phishing Detection

The results indicate that machine learning models, especially SVM, can greatly improve phishing detection systems. While Naive Bayes is efficient, it may fall short in accurately addressing complex phishing attack scenarios. Random Forest offers a balanced approach, performing effectively in real-world applications with high feature dimensionality.

V. CONCLUSION

This study highlights the effectiveness of machine learning algorithms—SVM, Naive Bayes, and Random Forest—in identifying phishing attacks. Among these, SVM achieved the highest accuracy and F1-score, while Random Forest and Naive Bayes also demonstrated encouraging results. These algorithms can be utilized to create automated phishing detection systems that enhance online user security. Future research could aim at incorporating these models into real-time web browsing scenarios and investigating more advanced methods, such as deep learning, to further boost detection accuracy.

REFERENCES

[1]. K. Jain, et al., "Phishing Website Detection Using Support Vector Machines," *International Journal of Computer Science and Engineering*, vol. 5, pp. 98-104, 2017.

[2]. D. Sharma, "A Comparative Study of Classification Algorithms for Phishing Detection," *Journal of Computer Security*, vol. 24, no. 3, pp. 112-130, 2018.

[3]. UCI Machine Learning Repository, "Phishing Website Dataset," [Online] Available: https://archive.ics.uci.edu/ml/datasets/phishing+websites.

DOI: 10.48175/IJARSCT-27577