Krrish Kumar, 2026, 14:2
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science, Engineering and Technology
An Open Access Journal

An Intelligent Phishing Website Detection System Using Machine Learning Algorithms

Krrish Kumar[1], Kumar Aryan[2], Akash Kumar[3], Kumar Divyanshu[4], Vinay Kumar Pant[5]

[1,2,3,4]Student of Department of Computer Application, Haridwar University, Roorkee, India
[5]Assistant Professor, Department of Computer Application, Haridwar University, Roorkee, India

Abstract- Phishing attacks are one of the most popular cyber threats, where attackers design a copy of a genuine website to steal confidential information like usernames, passwords, and bank account details. It is quite difficult for common users to identify genuine and phishing websites, resulting in loss of money and data breaches. This project work presents a Machine Learning-based phishing website detection system that examines the URL of the website as well as its HTML structure. It identifies features like URL length, number of links, forms, scripts and external resources. Different algorithms like Random Forest, Support Vector Machine (SVM), Decision Tree, Naive Bayes, and K-Nearest Neighbours (KNN) are used and compared. Among them, Random Forest gave the best accuracy. The system is automated, accurate, and able to identify new phishing websites, thus improving the security of online users.

Keywords: Phishing Detection, Machine Learning, Cyber Security, URL Analysis, Random Forest.

I. INTRODUCTION

The rapid growth of internet technology has increased the number of online services such as e-commerce, social media, cloud computing, and online banking. While these services improve user convenience, they also introduce various cybersecurity threats. One of the most dangerous and widespread cyber threats is phishing attacks [9, 12]. Phishing attacks involve fake websites that imitate legitimate and trusted websites to deceive users into sharing confidential information. These websites often mimic banks, payment gateways, email providers, and social media platforms. Users unknowingly provide their login credentials, credit card details, or personal information, which attackers later exploit for financial fraud or identity theft [10, 11].Traditional phishing detection techniques mainly rely on blacklist-based detection methods and manual verification systems. However, these approaches fail to detect newly generated phishing websites because attackers continuously create new domains and modify website structures.

Therefore, blacklist-based systems become ineffective against zero-day phishing attacks. Machine learning provides an effective solution to phishing detection. Machine learning models can learn patterns from historical datasets and detect suspicious characteristics of websites automatically. These models analyze both URL-based and content-based features to classify websites as phishing or legitimate [3].The objective of this research is to design and develop a machine learning-based phishing detection system that compares multiple algorithms and identifies the most accurate model for detecting phishing websites.

II. LITERATURE REVIEW

Mohammad et al. (2014) [1], proposed a phishing detection system using machine learning techniques that analyze both URL-based and content-based features. The authors applied algorithms such as Decision Tree and Random Forest. Their results demonstrated that machine-learning models could effectively detect phishing websites with high accuracy.

Abdelhamid et al. (2014) [2], introduced an associative classification-based phishing detection method using data mining techniques. Their system analyzed multiple website attributes and improved phishing detection accuracy compared to traditional blacklist approaches.

Sahingoz et al. (2019) [3], developed a phishing detection system based on URL features using

machine learning algorithms such as Random Forest, SVM, and Logistic Regression. Their results showed that Random Forest performed better than other algorithms in terms of accuracy and computational efficiency.

Jain & Gupta (2018) [4], proposed a client-side phishing detection approach using machine learning algorithms. Their method focused on detecting phishing websites without relying on third-party services, making the system more efficient and scalable.

Aljofey et al. (2020) [5], proposed a phishing detection system using deep learning techniques. The study analyzed both URL-based features and webpage content features to detect phishing websites. The researchers applied neural network models and achieved high detection accuracy. Their findings showed that deep learning models can significantly improve phishing detection performance compared to traditional machine learning algorithms.

Adebowale et al. (2021) [6], introduced a machine learning approach for detecting phishing websites using URL and domain-based features. The researchers implemented algorithms such as Random Forest, Support Vector Machine, and Gradient Boosting. Their results demonstrated that ensemble- learning models provided better accuracy and reliability in detecting phishing attacks.

Bahnsen et al. (2022) [7], proposed a phishing detection model based on real-time URL analysis. The research focused on extracting features from website URLs and applying machine learning classification techniques. The system was designed to detect phishing attacks in real-time and demonstrated improved performance compared to traditional blacklist-based detection methods.

III. RESEARCH GAP IDENTIFIED

- Many existing phishing detection systems focus only on URL-based features or content-based features, which may limit the overall accuracy of the detection model.
- Some studies use complex deep learning models, which require high computational resources and longer processing time, making them less suitable for real-time detection systems.
- Several research works evaluate their systems using only one or two machine learning algorithms, which does not provide a complete comparison of different classification techniques.
- In many cases, existing models are unable to effectively detect newly generated phishing websites, especially those that use advanced obfuscation techniques.

IV. PROPOSED METHODOLOGY

This research follows a quantitative experimental design to develop an intelligent phishing website detection system using machine learning algorithms. The methodology involves dataset collection, feature extraction, data preprocessing, model training, and performance evaluation. Multiple classification algorithms are used to determine the most accurate phishing detection model.

The following machine learning algorithms are implemented:

Random Forest:- Random Forest is a powerful machine learning algorithm that is based on the concept of Decision Trees. Instead of using a single tree, Random Forest creates multiple decision trees and combines their predictions to produce the final result [4, 5].

Support Vector Machine (SVM):- Support Vector Machine (SVM) is a supervised machine learning algorithm widely used for classification problems. The main objective of SVM is to find the best boundary that separates data points belonging to different classes. This boundary is known as a hyperplane. Each data point in the dataset is represented as a point in an n-dimensional space based on its features. SVM identifies the closest data points from each class, called support vectors, which help define the position of the hyperplane. The algorithm tries to maximize the margin between the hyperplane and support vectors [6, 7].

Decision Tree:- Decision Tree is one of the most commonly used algorithms in machine learning for classification tasks. It is simple to understand and easy to implement. The algorithm works by creating a tree-like structure where decisions are made based on different conditions. The process starts by selecting the best attribute from the dataset, which becomes the root node of the tree. The dataset is then divided into smaller subsets based on different attribute values. Each internal node represents an attribute, while each leaf node represents the final class label such as phishing or legitimate website. Methods like Gini Index and Information Gain are used to determine the best attribute for splitting the data[8].

Naive Bayes:- Naive Bayes is a probabilistic machine learning algorithm based on Bayes' Theorem. It is commonly used for classification tasks because it is fast and efficient. The algorithm assumes that all features in the dataset are independent of each other, which simplifies the calculation process. In phishing detection, Naive Bayes calculates the probability that a website belongs to a particular class based on its features such as URL structure, links, or scripts. Using these probabilities, the algorithm predicts whether a website is phishing or legitimate. Even though the independence assumption may not always be true, Naive Bayes still performs well in many real-world classification problems[9].

K-Nearest Neighbors (KNN):-K-Nearest Neighbors (KNN) is a straightforward machine learning technique for classification problems. The technique relies on finding the K data points closest to a new data point based on their distances, such as Euclidean distance. The technique classifies a new data point based on the class of its K nearest neighbors.In applying KNN for detecting phishing sites, features such as the length of URLs, age of domains, and suspicious links are compared with other sites. The technique classifies a website as a phishing or non-phishing site based on similarity. Although it is a time-consuming technique, it is successful in solving many classification problems[10].

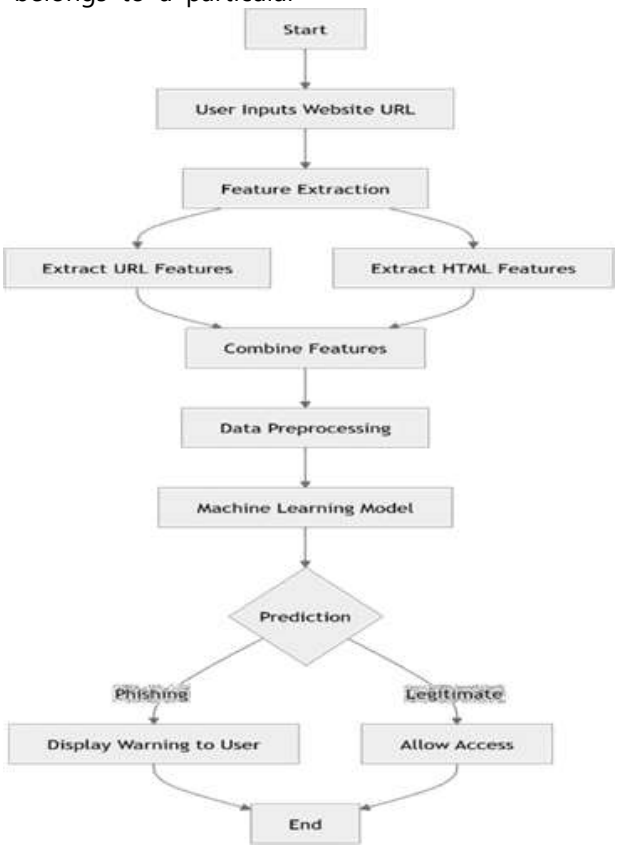

Fig.1. System Architecture

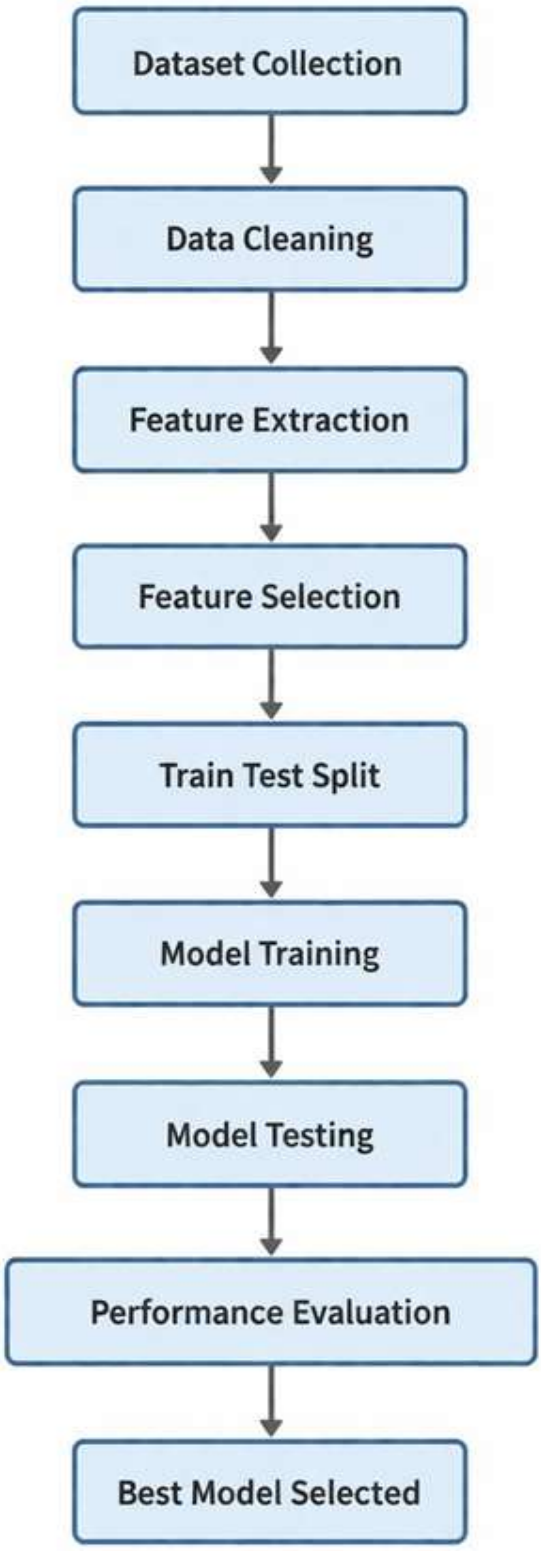

Fig.2. Proposed Phishing Detection Model

Dataset Collection

The dataset used for this research contains both phishing and legitimate website URLs. These datasets were collected from publicly available sources such as:

- PhishTank
- UCI Machine Learning Repository
- Kaggle phishing datasets

The dataset includes several attributes related to website structure and URL properties.

Feature Extraction

Table1 describe important features and feature description. These features help machine learning algorithms distinguish between legitimate and phishing websites[2].

Table1. Feature Description

Feature	Description
URL Length	Length of the website URL
Number of Dots	Indicates suspicious domains
HTTPS Usage	Secure protocol presence
External Links	Links pointing to external domains
Forms	Presence of login or input forms
JavaScript	Suspicious scripts
Redirects	Redirection behaviour

Data Preprocessing

Data preprocessing steps include:

- Removing missing values
- Feature scaling
- Encoding categorical features
- Splitting dataset into training and testing sets Typically:
- 80% Training Data
- 20% Testing Data

V. RESULTS AND PERFORMANCE EVALUATION

The performance of the machine learning models is evaluated using the following metrics:

- Accuracy
- Precision
- Recall
- F1-score

Model Accuracy Comparison

Table 2 shows Comparative accuracy results of machine learning algorithms for phishing website detection. The results show that Random Forest provides the best performance for phishing detection.

Table2. Accuracy Comparison table of various Algorithm

Algorithm	Accuracy
Decision Tree	92%
Naive Bayes	89%
KNN	91%
SVM	94%
Random Forest	97%

Bellow Fig.3 represent the Accuracy comparison chart of various algorithm. Random Forest has the highest accuracy (~97%), making it the best performer in this comparison. SVM is the second best with around 94% accuracy. Naive Bayes has the lowest accuracy (~89%). The chart indicates that random forest technique is better than other model, and the less complicated probabilistic models such as Naive Bayes are perhaps slightly inferior on this dataset.

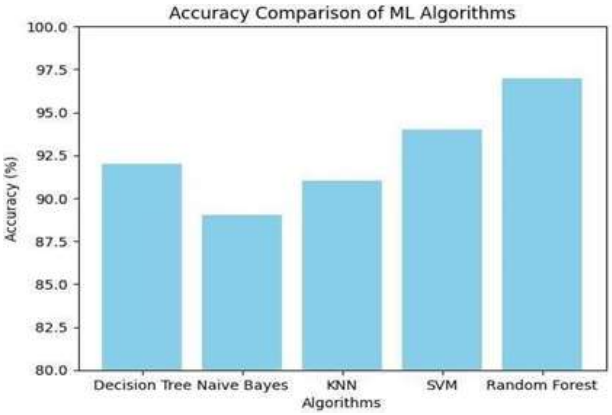

Fig 3. Accuracy Comparison Chart

Comparative Analysis

Different machine learning algorithms offer varying levels of accuracy, computational efficiency, and complexity. A comparative analysis of the algorithms used in this study is presented in Table 3. Random Forest achieved the best overall performance in this study.

Table 3. Comparative Analysis of Algorithm.

Algorithm	Advantages	Limitations
Decision Tree	Easy to interpret	Overfitting
Naive Bayes	Fast computation	Assumes feature independence
KNN	Simple implementation	Slow for large datasets
SVM	High accuracy	Computationally expensive
andom Forest	High accuracy, reduces overfitting	Slightly complex

VI. CONCLUSION

Phishing attacks continue to be one of the most serious threats to internet users and online systems. Traditional blacklist-based detection techniques are not sufficient because they are unable to detect newly created phishing websites. Therefore, more intelligent and automated detection methods are required.

In this research, a machine learning-based phishing website detection system was proposed. The system analyzes both URL-based features and HTML structure features of websites to identify phishing attempts.

Several machine learning algorithms such as Decision Tree, Random Forest, Support Vector Machine (SVM), Naive Bayes, and K-Nearest Neighbors (KNN) were implemented and compared to evaluate their performance.

Based on the experimental results, the Random Forest algorithm achieved the highest accuracy among the evaluated models. The results show that ensemble learning techniques can improve the reliability of phishing detection systems.

Overall, the proposed system provides an effective solution for detecting phishing websites and improving online security. In the future, this work can be extended by integrating deep learning models and real-time browser-based phishing detection

systems to further enhance detection accuracy and performance.

REFERENCES

1. Mohammad, R. M., Thabtah, F., & McCluskey, L. (2014). Predicting phishing websites based on selfstructuring neural network. Neural Computing and Applications, 25(2), 443–458.
2. Abdelhamid, N., Ayesh, A., & Thabtah, F. (2014). Phishing detection based associative classification data mining. Expert Systems with Applications, 41(13), 5948–5959.
3. Sahingoz, O. K., Buber, E., Demir, O., & Diri, B. (2019). Machine learning based phishing detection from URLs. Expert Systems with Applications, 117, 345–357.
4. Jain, A. K., & Gupta, B. B. (2018). Towards detection of phishing websites on client-side using machine learning based approach. Telematics and Informatics, 35(4), 1099–1113
5. 5. Aljofey, A., Jiang, Q., Rasool, A., Chen, H., & Liu, W. (2020). An effective phishing detection model based on character level convolutional neural networks. Electronics, 9(9), 1514.
6. Adebowale, M. A., Lwin, K. T., Hossain, M. A., & Santoso, S. (2021). Intelligent web- phishing detection and classification model using machine learning algorithms. Journal of Information Security and Applications, 58, 102709.
7. Bahnsen, A. C., Bohorquez, E., Villegas, S., Vargas, J., & Gonzalez, F. A. (2022). Classifying phishing URLs using recurrent neural networks. Computers & Security, 114, 102577.
8. Singh, A., & Mehta, P. (2023). Hybrid machine learning approach for phishing website detection using URL and content-based features. International Journal of Computer Applications, 185(15), 20–26.
9. Verma, R., & Das, A. (2017). What you see is not what you get: Detecting phishing websites using machine learning techniques. Proceedings of the ACM Conference on Data and Application Security, 1–28
10. Zhang, Y., Hong, J., & Cranor, L. (2020). CANTINA+: A feature-rich machine learning framework for detecting phishing web sites. ACM Transactions on Information and System Security, 21(3), 1–28.
11. Rao, R. S., & Pais, A. R. (2019). Detection of phishing websites using an efficient feature-based machine learning framework. Neural Computing and Applications, 31(8), 3851–3873.
12. Gupta, B. B., Arachchilage, N. A. G., & Psannis, K. E. (2021). Defending against phishing attacks: Taxonomy of methods, current issues and future directions. Telecommunication Systems, 67(2), 247– 267.