# Phishing Website Detection using Machine Learning Algorithms

Mrs.R.Amsaleka[1], Deepika M[2], Dharshini R[3], Induja S[4], Yogeshwari S[5]
*B.E-Computer Science and Engineering (Final year), Vivekanandha College of Technology for Women, Tamilnadu, India[1 2 3 4]*
*Assistant Professor, Computer Science and Engineering, Vivekanandha College of Technology for Women, Tamilnadu, India[5]*

**Abstract- Phishing attacks continue to pose significant threats to online users by mimicking legitimate websites to steal sensitive information. This paper presents a machine learning-based approach for the detection and classification of phishing websites using a combination of supervised learning algorithms. Various features, including URL characteristics, domain identity, and webpage content, are extracted and analyzed. The study evaluates the performance of classifiers such as Decision Tree, Random Forest, Support Vector Machine (SVM), and Logistic Regression on a benchmark phishing dataset. Experimental results demonstrate that ensemble models, particularly Random Forest, achieve superior accuracy and robustness in identifying phishing websites. The findings highlight the effectiveness of machine learning in enhancing web security through early detection and prevention of phishing attacks.**

**Keywords- Phishing attack, Machine learning**

## 1. INTRODUCTION

Phishing is a deceptive cyberattack technique in which attackers impersonate legitimate entities to trick users into disclosing sensitive information such as usernames, passwords, credit card numbers, and personal identification details. Typically executed through fake emails, instant messages, or fraudulent websites, phishing exploits human trust rather than technical vulnerabilities. According to recent cybersecurity reports, phishing accounts for a significant proportion of data breaches and financial fraud incidents globally, with attackers increasingly leveraging advanced evasion techniques, such as homograph domains and real-time content manipulation [1] The economic and reputational damage caused by phishing attacks continues to grow, making phishing detection a critical area of research in cybersecurity.

Traditional phishing detection mechanisms primarily rely on blacklist-based systems, signature matching, and manually defined heuristic rules. While these approaches are useful in identifying known phishing sites, they often fail to detect zero-day or rapidly mutating attacks due to their limited adaptability and reliance on previously encountered data. Moreover, the time lag between the emergence of a phishing website and its inclusion in a blacklist creates a vulnerability window for unsuspecting users [2]. Rule-based filters also suffer from high false positive rates, which can disrupt legitimate communications and reduce user trust in the detection system. Consequently, there is a strong need for more intelligent, scalable, and real-time detection techniques that can identify phishing threats based on underlying patterns and behaviors rather than fixed signatures.

In response to these limitations, machine learning (ML) has emerged as a promising solution for phishing detection. ML algorithms can learn from large datasets and uncover complex patterns that are not easily captured by static rules or human analysts. By extracting and analyzing a wide range of features— such as URL structures, domain registration details, HTML content, and third-party service usage—ML models can classify websites as phishing or legitimate with high accuracy. This paper investigates the effectiveness of several supervised machine learning algorithms, including Decision Tree, Random Forest, Support Vector Machine (SVM), and Logistic Regression, in detecting phishing websites [3]. The goal is to evaluate their performance using standard metrics such as accuracy, precision, recall, and F1-score, and

to demonstrate the feasibility of ML-based detection systems in enhancing online security.

## 2. LITERATURE REVIEW

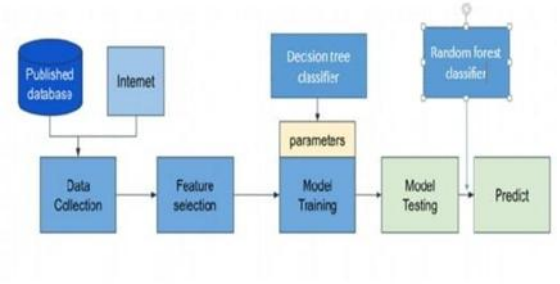
Many scholars have done some sort of analysis on the statistics of phishing URLs. Our technique incorporates key concepts from past research. We review past work in the detection of phishing sites using URL features, which inspired our current approach. Happy describe phishing as "one of the most dangerous ways for hackers to obtain users' accounts such as usernames, account numbers and passwords, without their awareness." Users are ignorant of this type of trap and will ultimately, they fall into Phishing scam. This could be due to a lack of a combination of financial aid and personal experience, as well as a lack of market awareness or brand trust. In thisarticle, Mehmet et al. suggested a method for phishing detection based on URLs. To compare the results, the researchers utilized eight different algorithms to evaluate theURLs of three separate datasets using various sorts of machine learning methods and hierarchical architectures. The first method evaluates various features of the URL; the second method investigates the website's authenticity by determining where it is hosted and who operates it; and the third method investigates the website's graphic presence. We employ Machine Learning techniques and algorithms to analyse these many properties of URLs and websites. Gareca et al. classify phishing URLs using logistic regression over hand-selected variables. The inclusion of red flag keywords in the URL, as well as features based on Google's Web page and Google's Page Rank quality recommendations, are among the features. Without access to the same URLs and features as our approach, it's difficult to conduct a direct comparison.

In this research, Yong et al. created a novel approach for detecting phishing websites that focuses on detecting a URL which has been demonstrated to be an accurate and efficient way of detection. To offer you a better idea, our new capsule- based neural network is divided into several parallel components. One method involves removing shallow characteristics from URLs. The other two, on the other hand, construct accurate feature representations of URLs and use shallow features to evaluate URL legitimacy. The final output of our system is calculated by adding the outputs of all divisions. Extensive testing on a dataset collected from the Internet indicate that our system can compete with other cutting-edge detection methods.

## 3. METHODOLOGY

A phishing website is a social engineering technique that imitates legitimate webpages and uniform resource locators (URLs). The Uniform Resource Locator (URL) is the most common way for phishing assaults to occur. Phisher has complete control over the URL's sub-domains. The phisher can alter the URL because it contains file components and directories. This research used the linear-sequential model, often known as the waterfall model. Although the waterfall approach is considered conventional, it works best in instances where there are few requirements. The application was divided into smaller components that were built using frameworks and hand-written code.

ARCHITECTURE DIAGRAM




## 4. DATASET

The UCI Phishing Websites Dataset (available at the UCI Machine Learning Repository) consists of 11,055 instances. The Phishing Detection Dataset on Mendeley, which contains 88,647 records with 31 features including HTTPS usage, IP presence, and URL characteristics. The Phish Tank Dataset offers over 1.5 million URLs (phishing and legitimate), providing up-to-date, real-world data but requiring significant preprocessing for use in machine learning models.

## 5. FEATURE EXTRACTION

We have implemented python program to extract features from URL. Below are the features that we have extracted for detection of phishing URLs.

1. URL-Based FeaturesThe URL is often the

first indicator of a phishing attempt. Analyzing its structure can reveal malicious intent:

Length of URL: Long URLs may obfuscate the actual destination.

Use of Suspicious Domains: Domains with unusual characters or misspellings.

Presence of HTTPS: Absence may indicate an insecure site.

Number of Subdomains: Excessive subdomains can be a red flag.

IP Address in URL: Direct IP addresses instead of domain names.

2. HTML-Based Features

The structure and content of a webpage provide insights into its legitimacy:

Presence of Forms: Forms requesting sensitive information are common in phishing sites.

JavaScript Usage: Excessive or hidden scripts may indicate malicious behavior.

iFrame Elements: Embedding other sites can be used to deceive users.

Redirect Behavior: Multiple redirects can be a tactic to mask the final destination.

3. WHOIS and DNS Features

Information about domain registration can indicate legitimacy:

Domain Age: Newly registered domains are often used for phishing.

Registrar Information: Lack of transparency may suggest malicious intent.

DNS Record Completeness: Missing records can be a warning sign.

4. Content-Based Features

The actual content of the webpage can be analyzed for phishing indicators:

Keyword Analysis: Presence of terms like "login", "verify", "account" in unusual contexts.

Textual Similarity: Comparison with known legitimate sites.

Multimedia Content: Use of logos or images to mimic trusted entities.

5. Behavioral Features

User interaction patterns can provide clues:

Mouse Movements: Tracking user behavior to detect anomalies.

Click Patterns: Unusual click sequences may indicate phishing.

Time Spent on Page: Rapid interactions can be a sign of automated phishing attempts.

## 6. MACHINE LEARNING ALGORITHM

Three machine learning classification model Decision Tree, Random forest and Support vector machine has been selected to detect phishing websites.

### 5.1 Decision Tree Algorithm [5]

A decision-making algorithm in machine learning is a method that helps a computer choose the best action or prediction based on data. These algorithms learn from past examples to improve their decisions over time. For example, a machine learning model can learn to decide whether an email is spam or not by studying many emails and their labels. Common decision- making algorithms in machine learning include decision trees, random forests, support vector machines, and neural networks. These algorithms look at patterns in the data and use them to make accurate predictions or choices. In simple terms, machine learning decision-making helps computers get better at making smart decisions by learning from experience.

### 5.2 Random Forest Algorithm [6]

Random Forest is a supervised machine learning algorithm used for classification and regression tasks. It works by creating multiple decision trees on random subsets of the training data and features, then combining their outputs through majority voting (for classification) or averaging (for regression). This ensemble approach increases accuracy and reduces overfitting compared to a single decision tree. In phishing website detection,

Random Forest effectively analyzes various features like URL structure, domain age, and security indicators to distinguish between phishing and legitimate websites with high accuracy.

### 5.3 Support Vector Machine Algorithm [7]

The Support Vector Machine (SVM) algorithm in machine learning is a powerful method used mainly for classification tasks, though it can also be used for regression. The main idea behind SVM is to find the best line (in 2D), plane (in 3D), or hyperplane (in higher dimensions) that separates data points from different classes. This line or plane is chosen so that it has the largest distance (called the *margin*) from the nearest data points of each class, which helps improve accuracy and reduce errors on new data.

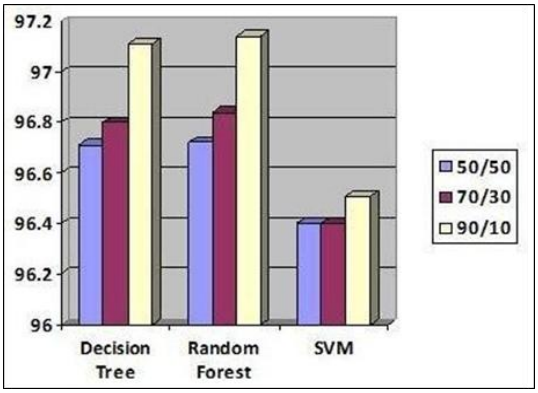



Fig. 1 Detection accuracy comparison

## 6. IMPLEMENTATION AND RESULT

Scikit-learn tool has been used to import Machine learning algorithms. Dataset is divided into training set and testing set in 50:50, 70:30 and 90:10 ratios respectively. Each classifier is trained using training set and testing set is used to evaluate performance of classifiers. Performance of classifiers has been evaluated by calculating classifier's accuracy score, false negative rate and false positive rate. Phishing is a very active and effective security threat that affects individuals as well as the targeted companies and organizations. Despite being around for many years, this threat is still one of the attack vectors most commonly used nowadays. The level of sophistication of the phishing campaigns has increased significantly over the years. Attackers employ numerous social engineering strategies and evasion techniques to make attacks more and more convincing for individuals and more challenging for detection tools. In this context research plays a critical role

**Table 1: Classifier's performance**

| Dataset Split ratio | Classifiers | Accuracy Score | False Negative Rate | False Positive Rate |
|---|---|---|---|---|
| 50:50 | Decision Tree | 96.71 | 3.69 | 2.93 |
| | Random Forest | 96.72 | 3.69 | 2.91 |
| | Support vector machine | 96.40 | 5.26 | 2.08 |
| 70:30 | Decision Tree | 96.80 | 3.43 | 2.99 |
| | Random Forest | 96.84 | 3.35 | 2.98 |
| | Support vector machine | 96.40 | 5.13 | 2.17 |
| 90:10 | Decision Tree | 97.11 | 3.18 | 2.66 |
| | Random Forest | 97.14 | 3.14 | 2.61 |
| | Support vector machine | 96.51 | 4.73 | 2.34 |

Result shows that Random Forest algorith1m gives better detection accuracy which is 97.14 with lowest false negative rate than decision tree and support vector machine algorithms.

Result also shows that detection accuracy of phishing websites increases as more dataset used as training dataset. All classifiers perform well when 90% of data used as training dataset.

Fig. 1 show the detection accuracy of all classifiers when 50%, 70% and 90% of data used as training dataset and graph clearly shows that detection accuracy increases when 90% of data used as training dataset and random forest detection accuracy is maximum than other two classifiers.

## CONCLUSION

This paper aims to enhance detection method to detect phishing websites using machine learning technology. We achieved 97.14% detection accuracy using random forest algorithm with lowest false positive rate. Also result shows that classifiers give better performance when we used more data as training data. In future hybrid technology will be implemented to detect phishing websites more accurately, for which random forest algorithm of machine learning technology and blacklist method will be used.

This survey presented various algorithms and

approaches to detect phishing websites by several researchers in Machine Learning.On reviewing the papers, we came to aconclusion that most of the work done by using familiar machine learning algorithms like Naïve Bayesian, SVM, Decision Tree and Random Forest.Some authors proposed a new system like Phish Score and Phish Checker for detection. The combinations of features with regards to accuracy, precision, recall etc. were used. Experimentally successful techniques in detecting phishing website URLs were summarized As phishing websites increases day by day, some features may be included or replaced with new ones to detect them.

REFERENCE


[1] P. Zhang, A. Oest, H. Cho, Z. Sun, R. Johnson, B. Wardman, S. Sarker, A. Kapravelos, T. Bao, R. Wang, Y. Shoshitaishvili, A. Doupé, and G.-J. Ahn, ‘‘CrawlPhish: Large-scale analysis of client-side cloaking techniques in phishing,’’ in Proc. IEEE Symp. Secur. Privacy (SP), May 2021, pp. 1109–1124

[2] Anti-Phishing Working Group—APWG. (2022). Phishing Activity Trends Report-1Q. [Online]. Available: https://docs.apwg.org/reports/apwg_trends_report_q1_2022.pdf

[3] A. Basit, M. Zafar, X. Liu, A. R. Javed, Z. Jalil, and K. Kifayat, ‘‘A comprehensive survey of AI-enabled phishing attacks detection techniques,’’ Telecommun. Syst., vol. 76, no. 1, pp. 139–154, Jan. 2021.

[4] Google Safe Browsing. Accessed: Oct. 10, 2022. [Online]. Available: https://safebrowsing.google.com/

[5] N. A. Azeez, S. Misra, I. A. Margaret, L. Fernandez-Sanz, and S. M. Abdulhamid, ‘‘Adopting automated whitelist approach for detecting phishing attacks,’’ Comput. Secur., vol. 108, Sep. 2021, Art. no. 102328.

[6] [6]. Khan, A. Ahmad, A. Qamar, M. Kamran, and M. Altaf, ‘‘SpoofCatch: A client-side protection tool against phishing attacks,’’ IT Prof., vol. 23, no. 2, pp. 65–74, Mar. 2021

[7] Y. Lin, R. Liu, D. M. Divakaran, J. Ng, Q. Chan, Y. Lu, Y. Si, F. Zhang, and J. Dong, ‘‘Phishpedia: A hybrid deep learning based approach to visually identify phishing webpages,’’ in Proc. 30th USENIX Secur. Symp., 2021, pp. 3793–3810.

[8] D.-J. Liu, G.-G. Geng, X.-B. Jin, and W. Wang, ‘‘An efficient multistage phishing website detection model based on the CASE feature framework: Aiming at the real web environment,’’ Comput. Secur., vol. 110, Nov. 2021, Art. no. 102421.

[9] P. L. Indrasiri, M. N. Halgamuge, and A. Mohammad, ‘‘Robust ensemble machine learning model for filtering phishing URLs: Expandable random gradient stacked voting classifier (ERG-SVC),’’ IEEE Access, vol. 9, pp. 150142–150161, 2021

[10] X. Xiao, W. Xiao, D. Zhang, B. Zhang, G. Hu, Q. Li, and S. Xia, ‘‘Phishing websites detection via CNN and multi-head self-attention on imbalanced datasets,’’ Comput. Secur., vol. 108, Sep. 2021, Art. no. 102372.

[11] B. Wei, R. A. Hamad, L. Yang, X. He, H. Wang, B. Gao, and W. L. Woo, ‘‘A deep-learning-driven light-weight phishing detection sensor,’’ Sensors, vol. 19, no. 19, Sep. 2019, Art. no. 4258.

[12] S. Al-Ahmadi and T. Lasloum, ‘‘PDMLP: Phishing detection using multilayer perceptron,’’ Int. J. Netw. Secur. Appl., vol. 12, no. 3, pp. 59–72, May 2020