

Phishing Detection Using Machine Learning

Keerthana K P*¹, Dr. Md .Irshad Hussain B*²

P.G. Student, Department of Master of Computer Applications, University BDT College of Engineering, Davangere-577004 Karnataka, India.

Asst. Professor Department of Master of Computer Applications, UBDT, Davangere-577004. Davangere, Karnataka, India.

ABSTRACT

Phishing attacks are one of the most common cybersecurity threats that aim to steal sensitive information such as usernames, passwords, and financial details. This research proposes a machine learning-based phishing detection system that analyses website features to classify them as phishing. The system uses URL-based and domain-based features such as URL length, HTTPS presence, and domain age. A random forest algorithm is implemented to improve detection accuracy. The results show that the proposed system achieves high accuracy and can effectively detect phishing websites, helping users stay safe online. Although many methods have been proposed to detect phishing websites, Phishers have evolved their methods to escape from these detection methods. One of the most successful methods for detecting these malicious activities is machine learning. In this paper, we compared the results of multiple machine learning methods for predicting phishing websites.

1.INTRODUCTION

With the rapid growth of internet usage, phishing attacks have become a major security concern. Attackers create fake websites that look similar to legitimate ones to trick users into

METHODOLOGY

Step 1: Dataset Collection

A dataset of phishing and legitimate URLs is collected from online sources.

Use phishing URLs from:

- ❖ phishTank
- ❖ Kaggle datasets
- ❖ Legitimate websites from Alexa/Google

Step 2: Feature Extraction

Important feature are extracted, including:

- ❖ URL length
- ❖ Presence of HTTPS
- ❖ Number of special characters
- ❖ Domain age
- ❖ Use of ip address instead of domain name

entering sensitive information. Traditional detection methods are not always effective in identifying new phishing attacks. Therefore, there is a need for an intelligent system that can detect phishing websites automatically. Machine techniques provide a powerful solution by learning patterns from data and identifying malicious websites efficiently. phishing is a type of cyberattack where attackers attempt to steal sensitive information such as usernames, passwords, credit card details, and personal data by impersonating legitimate organizations through fake websites, emails, or messages. Attackers continuously modify URLs, website structures, and content to bypass conventional security systems.

Machine Learning has emerged as an effective solution for phishing detection due to its ability to learn patterns or emails as phishing. ML algorithms can analyze various features such as URL length, domain age, and presence of suspicious symbols, website traffic, SSL certificates, and webpage content. Several machine learning algorithms such as decision tree, random forest, and support vector machine (SVM), naïve bayes, and neural networks have been widely used in phishing detection research. Deep learning techniques are also gaining popularity for detecting complex phishing patterns without manual feature engineering.

Step 3: Model Selection

The random forest algorithm is used for classification because it provides high accuracy and reduces overfitting.

Algorithms:

- ❖ Logistic Regression
- ❖ Decision Tree
- ❖ Random Forest
- ❖ Support Vector
- ❖ Machine
- ❖ XGBoost
- ❖ Naïve Bayes

Step 4: System Architecture

The system takes a URL as input, extracts features, and classifies it as phishing or legitimate using the trained model.

Advantages

- ❖ Fast detection
- ❖ Works on unknown phishing sites
- ❖ High accuracy
- ❖ Can be integrated into browsers

- ❖ Helps protect users instantly

KNN ALGORITHM

KNN Algorithm for Phishing Detection

Step 1: Data Collection

Collect a dataset of websites/email labeled as:

- **Phishing (1)**
- **Legitimate (0)**

Common datasets: URL-based phishing datasets.

Step 2: Feature Extraction

Convert raw data into features. Example features:

- URL length
- Presence of “@” symbol
- Number of dots in URL
- HTTPS usage
- Domain age
- Presence of IP address instead of domain

Step 3: Data Preprocessing

- Normalize features (important for KNN)
- Handle missing values
- Split dataset:
 - Training set (80%)
 - Testing set (20%)

Step 4: Choose K Value

Select number of neighbors:

- Small K → sensitive to noise
- Large K → smoother but slower

Step 5: KNN Algorithm Steps

Algorithm:

Input: Training data, Test data, K value

For each test sample:

1. Calculate distance between test sample and all training samples
(use Euclidean distance)

2. Sort distances in ascending order

3. Select top K nearest neighbors

4. Count class labels:

- Phishing (1)
- Legitimate (0)

5. Assign class with majority votes

Output: Predicted class

II. LITERATURE SURVEY

Phishing attacks are a major cybersecurity threat where attackers trick users into revealing sensitive information such as passwords, banking details, and personal data. Over the years, researchers have proposed various techniques to detect phishing websites and emails, ranging from traditional rule-based systems to advanced machine learning models.

Early approaches to phishing detection relied on **blacklists and heuristic-based methods**. These techniques compared URLs against known phishing databases or applied predefined rules such as checking URL length, presence of special characters, or suspicious domain names. However, these methods were limited because attackers continuously generate new phishing sites, making it difficult to maintain updated blacklists.

To overcome these limitations, researchers introduced **machine learning (ML) techniques**. ML models can automatically learn patterns from data and identify phishing attempts more effectively. Common algorithms used include **Decision Trees, Random Forest, Support Vector Machines (SVM), Naïve Bayes, and Logistic Regression**. These models analyze features such as URL structure, domain age, website content, and security indicators (e.g., HTTPS usage).

Several studies have demonstrated the effectiveness of ML-based approaches:

- Researchers found that **Random Forest and Decision Tree models** provide high accuracy due to their ability to handle large feature sets and nonlinear relationships.
- **Support Vector Machines (SVM)** have shown strong performance in classifying phishing and legitimate websites, especially with well-selected features.
- **Naïve Bayes classifiers** are efficient and fast, making them suitable for real-time phishing detection systems.

In recent years, **deep learning techniques** have gained attention. Models such as **Artificial Neural Networks (ANN), Convolutional Neural Networks (CNN), and Recurrent Neural Networks (RNN)** can automatically extract complex features from URLs and webpage content without manual feature engineering. These approaches improve detection accuracy but often require large datasets and higher computational resources.

Additionally, hybrid approaches combining **machine learning with feature selection techniques** and **natural language processing (NLP)** have been proposed to improve performance. These methods analyze textual content in emails and websites to detect phishing intent.

Despite advancements, challenges remain in phishing detection, including:

- Rapid evolution of phishing techniques
- Handling zero-day attacks (new, unseen phishing sites)
- Balancing accuracy and computational efficiency

Overall, the literature indicates that **machine learning-based phishing detection systems outperform traditional methods**, offering higher accuracy, adaptability, and scalability. However, continuous research is required to address emerging threats and improve real-time detection capabilities.

III. RESULTS



Figure 3.1: This login page provides secure access to the Phishing Detection System. Users can enter their username and password to log in and access the system's phishing detection features. The page also includes a Sign Up option for new users to create an account and use the application.

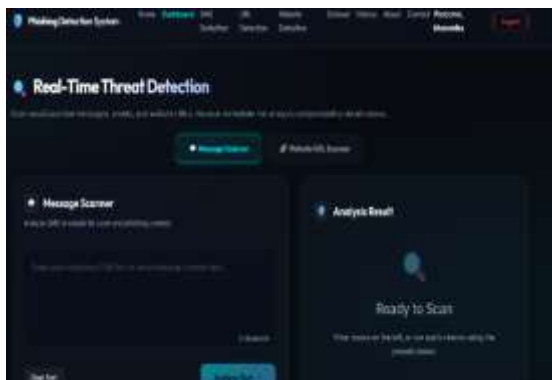


Figure 3.2: This dashboard serves as the main interface of the Phishing Detection System, enabling users to scan and analyze messages and URLs for phishing threats in real time. Users can enter suspicious content into the scanner, and the system displays the analysis results to help identify potential phishing attacks quickly and accurately.



Figure 3.3: The Website URL Scanner module allows users to enter a website link and analyze it for potential phishing threats. The system examines various URL features and security indicators to determine whether the website is safe or suspicious. The analysis result helps users identify malicious websites and avoid online scams.

IV. CONCLUSION

This research presents an effective phishing detection systems using machine learning. The system successfully identifies phishing websites with high accuracy. In the future, the system can be improve by using deep learning techniques and real-time detection mechanisms.

Machine learning provides an efficient and scalable solution for phishing website detection. Random forest and XGBoost show excellent performance with high accuracy and low false positives. Therefore, machine learning is a promising approach to improve cybersecurity defense systems.

V.REFERENCES

1. *Research papers from google scholar*
2. *Phishing datasets from online repositories.*