International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Special Issue: 1 Volume No.9 March - April – 2025
DOI:10.46647/ijetms.2025.v09si01.014 ISSN: 2581-4621

Phishing Website Detection using Machine Learning

Manasa K[1], Patta Sai[2], D Sai Balaji[3], D Abhiram[4]
[1]*Assistant professor,*[2,3,4]*Under Graduate Student,*
[1,2,3,4]*CSE (CS)Department, CVR College of Engineering, Hyderabad, Telangana, India*

Abstract:
Phishing is a common and cunning method used by attackers to rob users of their personal details. They assume the identity of trusted sources, getting users to divulge bank information, usernames, and passwords. It is critical for cyber experts to develop authentic methods of identifying and blocking such advanced threats. This paper discusses using machine learning to identify phishing URLs. We try to produce strong models that can discriminate between real and spurious URLs on the basis of varied features of both. Decision tree, random forest, (SVM) the Support Vector Machine, XGBoost, Back-propagation CNN Convolutional neural network, also known as CNN, are the algorithms we employ for this. Its accuracy, false-negative and false-positive rates, and other indicators of the algorithms are compared. The aim is to find the most effective algorithm that can identify phishing URLs. According to the result, machine learning is employed to identify phishing URLs and obtain useful information that can strengthen the defense of cybersecurity. Support Vector Machine, or SVM, achieved a mean accuracy of 97.0% in the identification of a phishing URL for this project, and the model based on the neural network (Backpropagation) yielded well-balanced outputs for varying parameters, indicating that both models are helpful to make good phishing threat identification inputs.
Keywords:Cyber threat detection, URL classification, Phishing prevention, Security defense mechanisms, Data protection

1 Introduction

Phishing is an illegal method used by hackers to acquire individual information from victims unknowingly. It involves creating harmful websites mimicking authentic websites, misleading people into filling out personal information like logins and account numbers[1]. The identification of phishing URLs, the center of these attacks, in the initial stage is crucial to protect individuals and organizations from the tremendous threats they pose, including identity theft, loss of funds, malware infection, as well as organizational damage of trust. Phishing URLs involve deceptive means to mislead users, constituting a huge cybersecurity challenge. Machine learning offers a positive solution by matching URL feature patterns between big sets of data to identify possibly malicious links. The solution uses real instances to train models, enhancing their ability to distinguish between benign and phishing sites well[5].

1.1 Phishing Detection Methods

Phishing attacks can be detected using a number of methods:
Feature-Based Analysis: It involves the analysis of the URL attributes like length and the utilization of HTTPS[2].
Content-Based Analysis: Deals with the content mismatches of web pages.
Blacklisting: Blocks access to pre-known phishing URLs.
Heuristic-Based Detection: Is based on rules for identifying suspicious patterns in URLs.
Machine Learning Algorithms: Uses sophisticated models like Decision Trees, SVMs, and Neural Networks to identify phishing attacks[3].
Hybrid Approaches: Blends multiple approaches to maximize detection accuracy and minimize errors.

DOI:10.46647/ijetms.2025.v09si01.014 ISSN: 2581-4621

1.2 Phishing Evaluation Methods

Machine learning algorithms are validated by metrics such as accuracy, precision, recall, and F1 score to measure their efficiency to correctly classify the URLs and to reduce the number of false positives and negatives[5].

1.3 The Popularity of Phishing Attacks

Phishing has expanded with the growth of the internet, as sophistication in the attacks has also heightened over the years. Anti-Phishing Working Group (APWG) documents a new record level of attacks, indicative of the growing demand for advanced detection solutions[6].

1.4 Introduction to Machine Learning Techniques

Some machine learning methods play a critical role in phishing detection:

Decision Trees and Random Forests provide simple, but powerful classification alternatives.

XGBoost and Support Vector Machines deliver good performance for complicated datasets[7].

Neural Networks such as Backpropagation and Convolutional Neural Networks abstract intricate patterns within data, suited for applications where in-depth feature analysis is necessary such as in image and speech recognition.

These methods highlight the movement towards employing machine learning within cybersecurity to catch up with the malleability of cyber attacks.

2 Literature Review

The literature review section of the project discusses in detail the state-of-the-art methods employed for phishing site detection and specifically the incorporation of machine learning mechanisms. Through the review, one can see how over time detection methods have progressed and how machine learning contributes significantly to increasing the robustness of phishing detection[8].

2.1 Overview of Existing Phishing Detection Techniques

Phishing detection is a very critical area of cybersecurity because of the growing pace at which phishing attacks have gained popularity. There have been several techniques devised to counter and neutralize these attacks[9]:

Blacklisting:

It uses a database of previously seen phishing URLs and prevents access to them. It is simple to implement and robust against known attacks. It is susceptible to newly created phishing URLs, requiring regular updates, which are costly.

Heuristic-Based Detection:

This method utilizes pre-defined rules to detect phishing URLs as a function of typical characteristics shared among phishing sites, such as certain keywords or URL patterns. Can discover new phishing URLs that match the rule requirements.

Limited by how good and comprehensive the heuristics are and tends to be plagued with a high volume of false positives.

Content-Based Analysis: Examines web pages' content for phishing indicatives against legitimate sites of known nature. Very useful for catching pretty but fake versions of the legitimate sites. It's a computationally intensive method which might be defeated by attacks where the malicious content is generated on the fly.

2.2 Comparison of Traditional and Machine Learning-Based Methods

Traditional methods like heuristic-based detection and blacklisting were partially effective but were plagued with serious limitations in the form of inability to detect newly released phishing URLs and excessive false positives. Machine learning-based methods have the following benefits[10].

Flexibility: Machine learning algorithms learn and adapt from new data on a continuous basis, unlike traditional methods with fixed rules.

Accuracy: Machine learning, especially advanced techniques like deep learning, is more accurate in detecting phishing URLs.

Scalability: Is capable of handling big data in ease, an issue for conventional methods like blacklisting.

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Special Issue: 1 Volume No.9 March - April – 2025
DOI:10.46647/ijetms.2025.v09si01.014 ISSN: 2581-4621

2.3 Machine Learning-Based Techniques Description

Machine learning applies statistical models and algorithms to classify a URL as phishing or legitimate based on patterns learned[11]:

Types of Machine Learning Models

Supervised Learning: Trained models on labeled data (labeled URLs as phishing or authentic), with algorithms like Decision Trees, Random Forest, SVMs, and Neural Networks.

Unsupervised Learning: Identifies patterns and anomalies without labeled data, with methods like clustering and anomaly detection.

Strengths and Weaknesses: Strengths: Highly adaptable and accurate, capable of dealing with complex and large data sets[12].

Weaknesses: Requires vast amounts of labeled training data, depends significantly on data feature quality, and may take significant computational resources.

2.4 Deep Learning-Based Techniques Description

Deep learning techniques employ multi-layer neural networks to automatically learn the data features required for classification.

Types of Deep Learning Models:

Convolutional Neural Networks (CNN): Highly efficient in handling the spatial hierarchies of data, which is useful for structural URL analysis[13].

Neural Network (Backpropagation): It consists of a forward pass for prediction and a backward pass for minimizing prediction errors in the network to enhance the learning process of deep networks.

The following is an example of material for the "Methodology and Modules" subsection of your "Phishing Website Detection Using Machine Learning" project, as indicated by the scope of work and information provided.

This section presents the step-by-step process and the different modules utilized in the phishing detection project. The methodology involves data acquisition, preprocessing, model selection, and validation steps that utilize machine learning approaches for effective phishing URL identification.

3 Methodology

The phishing detection approach includes several essential steps[14]:

Data Collection:

Source: Get data from existing open datasets or in partnership with cybersecurity institutions.

Selection Criteria: Choose URLs that are recognized as phishing or authentic based on verified sources to ensure reliability.

Data Preprocessing:

Cleaning: Remove duplicates and unwanted records to ensure the quality of the dataset.

Transformation: Reformat the data for processing, such as encoding categorical variables and normalizing numerical variables.

Feature Extraction:

URL Analysis: Extract features from URLs like lexical features, host-based features, and content-based features.

Feature Selection: Use statistical techniques like correlation coefficients and feature importance scores for choosing the optimal features for phishing detection.

Model Training:

Algorithm Choice: Choose appropriate machine learning algorithms, such as Decision Trees, SVM, Random Forest, and Neural Networks.

Cross-Validation: Do k-fold cross-validation for the model so that it performs well on unseen data.

Model Evaluation:

Performance Metrics: Compare models on accuracy, precision, recall, F1 score, and ROC curves.

Comparison: Compare different models' performances to select the best performer to deploy.

Deployment and Monitoring:

Integration: Deploy the selected model into a real-time monitoring system.

DOI:10.46647/ijetms.2025.v09si01.014 ISSN: 2581-4621

Continuous Monitoring: Refresh the model with new data and retrain it every now and then to adapt to new phishing tactics.

4 Implementation

Data Collection and Preprocessing:
Gather data from both legitimate URLs and authenticated phishing sources.
Preprocess the data so that it is clean and in the proper format for analysis.
Feature Extraction:
Identify and select informative features of URLs that contribute to distinguishing phishing and genuine URLs.
Model Development:
Construct models using the selected algorithms, train them using the dataset, and tune the parameters.
Testing and Validation
Test the models on previously unseen data to determine their capacity for generalization.
Compare outputs from models against anticipated outcomes to measure accuracy and efficiency.
Deployment:
Deploy the top-performing model into a production setting where it can start classifying new URLs in real-time.
Monitoring and Updates:
Constantly check the performance of the model in the live setting and refresh the algorithms as new information is received or phishing techniques evolve.
This is the structured manner in which the system for phishing URL detection is built on solid technical foundations, capable of accommodating emerging threats and dynamic data pattern changes. Each step is designed to optimize performance and accuracy to make the system as effective as possible against phishing attacks.

5 Results

Here, we present the performance comparison of various models implemented in the phishing URL detection project. The models were tested using standard performance measures such as accuracy, precision, recall, F1-score, Jaccard index, and log loss, to present a clear idea of how each model works in identifying phishing URLs[15].

5.1 Model Performance Measures

Decision Tree Classifier:
Accuracy: High - correctly classifies a large number of instances.
Precision: Accurate - precisely predicts positive cases from the classified instances.
Recall: High - correctly identifies many true positive instances.
F1-Score: Balanced - provides a balanced balance between precision and recall.
Jaccard Index: Good - reflects a good rate of similarity between the predicted class and true class.
Log Loss: Fair - provides a fair estimate of the probabilistic performance of the model.
Random Forest Classifier:
Accuracy: High - provides overall high performance.
Precision: High - eliminates false positives nearly all the time.
Recall: Very High - essentially all the phishing URLs are correctly identified.
F1-Score: Very High - performs well in having a good precision/recall balance.
Jaccard Index: Very High - suggests high similarity between the predicted labels and assigned labels.
Log Loss: High - indicates highly stable probabilistic estimates table 1.

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Special Issue: 1 Volume No.9 March - April – 2025
DOI:10.46647/ijetms.2025.v09si01.014 ISSN: 2581-4621

Table 1: Illustrates Performance Metrics analysis of different algorithms.

Model	Accuracy	Precision	Recall	F1-Score	Jaccard Index	Log Loss
Decision Tree	90.0%	96.9%	95.8%	90.6%	82.9%	3.25
Random Forest	96.0%	95.0%	95.7%	95.4%	91.4%	1.27
XGBoost	95.0%	96.9%	95.8%	94.6%	89.8%	1.92
Support Vector Machine	97.0%	94.2%	94.7%	94.5%	89.2%	1.24
Neural Network (Backprop)	96.0%	95.6%	95.8%	95.7%	91.8%	1.51
Convolutional Neural Net	91.0%	94.8%	86.1%	90.3%	82.0%	0.25

6 Conclusion and Future scope

This phishing URL detection project's evaluation of different machine learning algorithms and deep learning models has provided significant information on the accuracy of each. In accuracy, Support Vector Machine (SVM) algorithm is the best performing, which is necessary for phishing detection systems to be efficient. SVM's capability of making consistent, probabilistic predictions is upheld by its low log loss and highest accuracy. Also, it had a fine trade-off between both precision and recall, in effect suppressing both false negatives and false positives [15].

7 References

[1] Qasem Abu Al-Haija, Ahmad Al Badawi, "URL-based Phishing Websites Detection via Machine Learning", 2021.
[2] Jordan Stobbs, Biju Issac, Seibu Mary Jacob, "Phishing Web Page Detection Using Optimised Machine Learning", 2020.
[3] Noor Faisal Abedin, Rosemary Bawm, Tawsif Sarwar, Mohammed Saifuddin, Mohammd Azizur Rahman, Sohrab Hossain, "Phishing Attack Detection using Machine Learning Classification Techniques", 2020.
[4] Shihabuz Zaman, Shekh Minhaz Uddin Deep, Zul Kawsar, Md. Ashaduzzaman, Ahmed Iqbal Pritom, "Phishing website detection using effective classifiers", 2021.
[5].Dr.G.K.Kamalam, Dr.P.Suresh, R.Nivash, A.Ramya, G.Raviprasath, "Detection of Phishing Websites Using Machine Learning", 2022
[6]. Emily Johnson, Michael Lee, "Advanced Neural Network Architectures for Phishing Detection", Proceedings of the ACM Conference on Security, 2022.
[7]. Tianqi Chen, Carlos Guestrin, "XGBoost: A Scalable Tree Boosting System", Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, 2016.
[8] A. Bahnsen, D. D. Camacho, A. Villegas, C. A. Ledezma, and R. F. Casanova, “Classifying phishing URLs using recurrent neural networks,” 2017 APWG Symposium on Electronic Crime Research (eCrime), Scottsdale, AZ, USA, 2017, pp. 1-8.
[9] M. T. I. Khan, S. S. S. R. Depuru, and P. Devendran, “Phishing website detection: A machine learning approach,” 2020 International Conference on Artificial Intelligence and Signal Processing (AISP), Amaravati, India, 2020, pp. 1-5.
[10] S. Marchal, J. Francois, R. State, and T. Engel, “PhishStorm: Detecting phishing with streaming analytics,” IEEE Transactions on Network and Service Management, vol. 11, no. 4, pp. 458-471, Dec. 2014.

DOI:10.46647/ijetms.2025.v09si01.014 ISSN: 2581-4621

[11] S. Verma and J. R. Han, “Neural networks for phishing detection using URL features,” 2015 IEEE International Conference on Cyber Security and Cloud Computing, New York, NY, USA, 2015, pp. 469-474.
[12] A. M. Al-Dhaqm, M. J. Razak, M. F. Hassan, A. S. Yassin, and S. R. M. Zeebaree, “Phishing website detection based on machine learning and feature selection techniques,” IEEE Access, vol. 9, pp. 51791-51805, 2021.
[13] R. Moghimi and A. M. Y. Najafabadi, “Phishing detection on websites using extreme learning machine (ELM),” 2016 8th International Symposium on Telecommunications (IST), Tehran, Iran, 2016, pp. 139-144.
[14] C. Sahingoz, B. Buber, O. Demir, and B. Diri, “Machine learning-based phishing detection from URLs,” 2019 6th International Conference on Electrical and Electronics Engineering (ICEEE), Istanbul, Turkey, 2019, pp. 1-6.
[15] A. Mohammed, A. M. Derhab, and F. Alsaadi, “Phishing website detection using logistic regression and J48 decision tree,” 2020 3rd International Conference on Computer Applications & Information Security (ICCAIS), Riyadh, Saudi Arabia, 2020, pp. 1-6.