International Journal of Scientific Research & Engineering Trends
Volume 12, Issue 2, Mar-Apr-2026, ISSN (Online): 2395-566X

A Novel Ensemble Machine Learning Method to Detect Phishing Attack

Dr. Pawan Bhaladhare , Vaibhav Ingle, Sakshi Phatake, Rushi Jagtap
Department Of Computer Science Engineering
Sandip University, Nashik

Abstract- — The rapid growth of internet users has led to an increase in phishing attacks, where attackers create deceptive URLs to steal sensitive information. This study presents an ensemble machine learning framework for detecting phishing websites using Natural Language Processing (NLP) and multiple classifiers, including Artificial Neural Networks (ANN), Naïve Bayes (NB), Random Forest (RF), and Support Vector Machines (SVM). By extracting key features from URLs and applying machine learning techniques, the proposed model enhances detection accuracy. Comparative analysis demonstrates its effectiveness, achieving 98.4% accuracy in distinguishing phishing sites from legitimate ones. This approach offers a proactive solution to mitigate online security threats and protect users from cyber fraud. Phishing attacks have become more sophisticated, using deceptive URLs to target unsuspecting users. This research introduces a hybrid machine learning-based detection model that enhances accuracy through an ensemble of classifiers. The system utilizes Natural Language Processing (NLP) to extract critical URL features, which are then analyzed using Artificial Neural Networks (ANN), Naïve Bayes (NB), Random Forest (RF), and Support Vector Machines (SVM). Machine learning techniques are particularly effective in detecting zero-hour phishing attacks and adapting to emerging threats. Our implementation achieved a 98.4% accuracy in classifying websites as phishing or legitimate.

Keywords: Cyberattacks, Phishing Detection, Phishing URLs, Web Threat, Machine Learning Classifiers.

I. INTRODUCTION

n today's digital landscape, cybersecurity is a major concern, as a single attack can result in severe data breaches and financial losses. The growing use of smart devices has further expanded security vulnerabilities. Among various cyber threats, phishing remains one of the most widespread and effective tactics used by attackers. Phishing websites play a crucial role in online social engineering, where cybercriminals mimic legitimate sites to steal sensitive information such as login credentials, banking details, and personal data. The frequency of phishing attacks has surged in recent years, with a notable rise during the first half of 2020, particularly targeting widely used online services. A striking example of the rise in phishing attacks was the surge targeting the video conferencing platform Zoom, which became crucial for remote work and communication during the COVID-19 pandemic. According to the Anti-Phishing Working Group (APWG), phishing cases related to Zoom jumped from just eight in March 2020 to over 1,000 by April. This sharp increase underscores the evolving nature of phishing tactics and the urgent need for advanced detection mechanisms.

Phishing attacks typically occur through three primary methods: deceptive emails, fraudulent websites, and malicious social media campaigns. Cybercriminals craft misleading emails, text messages, or social media links that appear to come from legitimate sources, tricking users into disclosing sensitive information. Large-scale phishing campaigns increase the likelihood of success, making the development of advanced detection strategies essential.

This research explores machine learning-based techniques to detect phishing URLs and strengthen cybersecurity defenses against such threats. Cybersecurity, also known as information technology security, involves safeguarding computers, networks, and data from unauthorized access and cyberattacks. It encompasses system protection, disaster recovery, and user awareness training. The primary objective is to prevent data breaches and security threats that could compromise personal, corporate, and governmental information.

II. LITERATURE SURVEY:

2.1 Phishing Detection Using URL Blacklisting

Authors: J. Rashid, T. Mahmood, M. W. Nisar, and T. Nazir
This study presents a phishing detection system that alerts users about blacklisted URLs, preventing access to fraudulent websites. The system captures suspicious URLs, verifies legitimacy, and notifies users via pop-ups and email alerts. While this enhances security awareness, its reliance on static

blacklists limits effectiveness against evolving phishing threats. Machine learning- based approaches offer greater adaptability in detecting new phishing tactics.

2.2 Machine Learning-Based Phishing Detection in Web Browsers

Authors: A. Razaque, M. B. H. Frej, D. Sabyrov, A. Shaikhyn, F. Amsaad, and A. Oun

This research introduces a Google Chrome extension for phishing detection, developed using JavaScript. The system combines blacklisting with semantic analysis to identify phishing patterns based on textual content, links, and images. While effective, its broad feature set increases computational complexity, potentially affecting real-time performance.

2.3 Machine Learning Approach for Phishing Website Detection

Authors: M. M. Vilas, K. P. Ghansham, S. P. Jaypralash, and P. Shila

This study employs Extreme Learning Machine (ELM) for phishing detection, analyzing 30 key features such as URL structure, domain authority, and website legitimacy. While providing valuable insights, the model demonstrates lower accuracy compared to Adaptive Probabilistic Estimation (APE)- based methods, limiting its effectiveness.

2.4 Intelligent Phishing Detection Using Random Forest

Authors: B. Alswailem, N. Alabdullah, N. Alrumayh, and A. Alsedrani

This research proposes a browser-based phishing detection system using the Random Forest algorithm. By selecting 26 key phishing indicators, the model improves classification accuracy. However, limitations in handling low-ranging values impact accuracy and increase execution time, highlighting the need for optimization .

2.5 Deep Learning-Based Phishing URL Detection

Authors: S. Gupta, A. K. Verma, and P. K. Chaurasia

This study explores a deep learning approach for phishing detection using Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) to analyze URL structures and webpage content. The model leverages both lexical and host-based features, significantly improving accuracy compared to traditional machine learning models. However, its dependency on high computational power may limit real-time deployment in resource-constrained environments.

III. PROPOSED METHOD

Our project presents a novel machine learning-based framework for detecting phishing websites. Unlike traditional methods that rely on blacklists, our approach identifies new phishing URLs in real time, offering stronger protection against evolving threats.

The detection model classifies URLs based on key features, selecting seven critical parameters from 29 identified characteristics to enhance accuracy and overcome limitations in existing systems:

- SSLfinal_State – Checks if the website has a valid SSL/TLS certificate, a key security indicator.
- URL_of_Anchor – Evaluates the legitimacy of anchor tags within the webpage.
- Web_traffic – Analyzes site popularity and visitor traffic to assess credibility.
- Having_Sub_Domain – Detects misleading subdomain structures commonly used in phishing attacks.
- Links_in_Tags – Assesses the nature and number of links embedded in HTML elements.
- Prefix_Suffix – Identifies the use of hyphens or separators in domain names, a common phishing tactic.
- Request_URL – Verifies if external resources are loaded from untrusted domains.

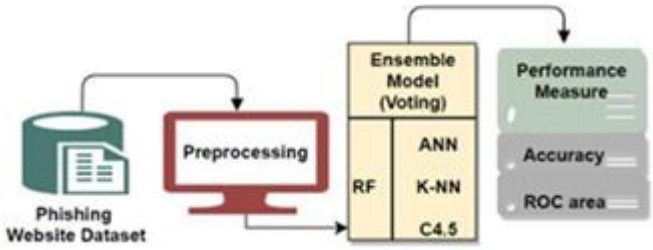

Fig 1. Proposed Method

The diagram illustrates a phishing website detection system using machine learning. The process consists of the following key steps:

1. Phishing Website Dataset

- The system begins with a dataset containing phishing and legitimate website URLs, along with relevant features.
- This dataset serves as input for training and testing the model.

2. Data Preprocessing

- Raw data is cleaned by handling missing values, removing inconsistencies, and transforming features into a machine-learning-friendly format.
- This step ensures high-quality, well-structured data for training.

3. Ensemble Model with Voting Mechanism

The system integrates multiple machine learning classifiers to improve phishing detection accuracy:

- Random Forest (RF): A decision tree-based approach that enhances prediction reliability.
- Artificial Neural Networks (ANN): Captures complex patterns using deep learning.
- K-Nearest Neighbors (K-NN): A distance-based classifier that groups similar data points.
- C4.5: A decision tree algorithm used for classification tasks.

A voting mechanism combines predictions from all models to make the final classification decision, improving overall accuracy.

4. Performance Evaluation

The model's effectiveness is assessed using key performance metrics:

- Accuracy: Measures the proportion of correctly classified phishing and legitimate websites.
- ROC Area (Receiver Operating Characteristic): Evaluates the model's ability to distinguish between phishing and legitimate websites using true positive and false positive rates.

IV. RESULT AND DISCUSSION

1. Experimental Setup

This section describes the experimental setup for applying machine learning algorithms to phishing website datasets. The configurations used for different algorithms are outlined in Table1. The experiments were conducted to detect phishing attacks by training and testing multiple machine learning models.

Table 1: Machine Learning Algorithm Configurations

Algorithm	Parameters	Value
RF	No. of estimators	100
	Criterion	Gini
	Max depth	None
	Random state	42
DT	Criterion	Entropy
	Max depth	None
	Random state	42
MLP	Solver	lbfgs
	Hidden layer sizes	100
	Activation function	relu
	Random state	42
XGB	Learning rate	0.1
	No. of estimators	100
	Random state	42
AdaBoost	Learning rate	1.0
	No. of estimators	50
	Algorithm	SAMMER.R
	Random state	42
GB	Learning rate	0.2
	No. of estimators	200
	Random state	42
Voting classifier	Estimators	RF, XGB, MLP
	Vote type	Hard

Before training the models, the dataset was split into training and testing sets. The training dataset accounted for 90% of the total data, while the remaining 10% was used for testing and performance evaluation.

2. Experimental Results

Experiments were conducted using six machine learning algorithms—Random Forest (RF), Decision Tree (DT), Multi-Layer Perceptron (MLP), Extreme Gradient Boosting (XGB), AdaBoost, and Gradient Boosting (GB). The models were tested on two phishing datasets in the Anaconda environment for binary classification. The performance was evaluated using four key

metrics: accuracy, precision, recall, and F1-score. The results were then compared with those of the Voting Classifier.

2.1 Results for the First Dataset

The performance metrics for each model on the first dataset are illustrated in Figure 1 and Table 2. The Voting Classifier outperformed the other models with the highest accuracy (0.978), precision (0.975), recall (0.987), and F1-score (0.981).

Model	Accuracy	Precision	Recall	F1-score
DT	0.964	0.961	0.976	0.968
RF	0.970	0.964	0.984	0.974
GB	0.960	0.959	0.971	0.965
XGB	0.973	0.976	0.976	0.976
AdaBoost	0.934	0.934	0.950	0.942
MLP	0.970	0.971	0.976	0.974
Voting	0.978	0.975	0.987	0.981

Fig. 2: Performance results–first dataset

2.2 Results for the Second Dataset

The results for the second dataset showed consistent performance across all models. Each algorithm demonstrated effective phishing detection capabilities based on the four evaluation metrics. The findings indicate that the models can successfully classify phishing websites with high accuracy.

Model	Accuracy	Precision	Recall	F1-score
DT	0.964	0.961	0.976	0.968
RF	0.970	0.964	0.984	0.974
GB	0.960	0.959	0.971	0.965
XGB	0.973	0.976	0.976	0.976
AdaBoost	0.934	0.934	0.950	0.942
MLP	0.970	0.971	0.976	0.974
Voting	0.978	0.975	0.987	0.981

Fig. 3: Performance results–Second dataset

V. CONCLUSIONS AND FUTURE WORK:

Phishing attacks are becoming more sophisticated, posing serious risks to users and online platforms. This study implements machine learning techniques to improve phishing detection accuracy. Using two datasets, we evaluated seven machine learning algorithms for website classification and phishing identification. Results showed that the XGBoost (XGB) algorithm outperformed other models in the first dataset, achieving high accuracy, precision, recall, and F1-score. In contrast, all models performed consistently well in the second dataset, demonstrating their reliability in phishing detection.

As phishing techniques evolve, traditional detection methods become less effective. Our findings confirm that machine learning, particularly XGB, is highly effective, achieving 0.978 accuracy in the first dataset. The consistent performance across models in the second dataset further validates their robustness.

Future Scope:

To further enhance detection capabilities, future work will focus on:

- Integrating deep learning for improved accuracy.
- Applying feature selection techniques to refine model performance.
- Enhancing ensemble models for better generalization.
- Exploring advanced data preprocessing methods to improve adaptability.

REFERENCES

1. A. R. Javed, M. O. Beg, M. Asim, T. Baker, and A. H. Al-Bayatti, “Alphalogger: Detecting motion-based side-channel attack using smart phone keystrokes,” Journal of Ambient Intelligence and Humanized Computing, pp. 1–14, 2020.
2. M. Mittal, C. Iwendi, S. Khan, and A. Rehman Javed, “Analysis of security and energy efficiency for shortest route discovery in low energy adaptive clustering hierarchy protocol using levenberg-marquardt neural network and gated recurrent unit for intrusion detection system,” Transactions on Emerging Telecommunications Technologies, p. e3997, 2020.
3. A. Rehman Javed, Z. Jalil, S. Atif Moqurrab, S. Abbas, and X. Liu, “Ensemble adaboost classifier for accurate and fast detection of botnet attacks in connected vehicles,” Transactions on Emerging Telecommu nications Technologies, p. e4088, 2020.
4. A. Rasool and Z. Jalil, “A review of web browser forensic analysis tools and techniques,” Researchpedia Journal of Computing, 2020.
5. “Phishing activity trends report,” https://docs.apwg.org//reports/apwg trends report q4 2016.pdf, 2020, accessed: 28-Aug-2020.
6. Z. Dong, A. Kapadia, J. Blythe, and L. J. Camp, “Beyond the lock icon: real-time detection of phishing websites using public key certificates,” in APWG Symposium on Electronic Crime Research (eCrime). IEEE, 2015, pp. 1–12.
7. C. Iwendi, Z. Jalil, A. R. Javed, T. Reddy, R. Kaluri, G. Srivastava, and O. Jo, “Keysplitwatermark: Zero watermarking algorithm for software protection against cyber-attacks,” IEEE Access, vol. 8, pp. 72650 72660, 2020.
8. A. Muhammad, M. Asad, and A. R. Javed, “Robust early stage botnet detection using machine learning,” EasyChair, Tech. Rep., 2020.

9. "Phishing activity trends report," https://docs.apwg.org/reports/apwg trends report q3 2019.pdf, 2020, accessed: 28-Aug-2020.
10. "Phishing activity trends report," https://docs.apwg.org/reports/apwg trends report q1 2020.pdf, 2020, accessed: 28-Aug-2020.