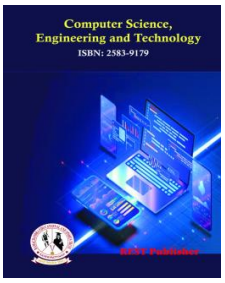
Computer Science, Engineering and Technology

Vol: 3(1), March 2025

REST Publisher; ISSN: 2583-9179 (Online)

Website: https://restpublisher.com/journals/cset/

DOI: https://doi.org/10.46632/cset/3/1/2



Detecting Phishing Websites Using Machine Learning

Rithika Mejole X M

Noorul Islam Centre for Higher Education, College in Kumarakovil, Tamil Nadu, India.

Corresponding Author Email: rithikamejole2001@gmail.com

Abstract: Phishing attacks, which trick users into divulging private information like passwords, credit card numbers, and personal information, have grown to be a serious cybersecurity risk. Blacklists and rule-based systems are examples of traditional security solutions that frequently fail to stop increasingly popular phishing websites. This study investigates how machine learning approaches can be used to identify phishing websites based on a variety of variables, including domain-based attributes, HTML content, and URL characteristics. Decision Trees, Random Forest, Support Vector Machines (SVM), and deep learning techniques are among the classification models that are trained using a dataset that includes both authentic and fraudulent websites. The accuracy, precision, recall, and F1-score measures are used to assess these models' performance. Results from experiments show that machine learning algorithms are capable of accurately and reliably classifying phishing websites, offering a scalable and reliable web security solution.

Keyword: Phishing Attacks, Cybersecurity, Deep Learning and Ineffective

1. INTRODUCTION

Malicious actors frequently employ phishing, a type of cyberattack, to trick users into disclosing private information including credit card numbers, login credentials, as well as personal information. Phishing assaults have become far more common in recent years, affecting people and organisations all around the world, according to the Anti-Phishing Working Group (APWG) [1]. Because attackers regularly alter their strategies to avoid detection, traditional phishing detection techniques like rules-based strategies and blacklists find it difficult to keep up with the quick rise of new phishing websites [2].

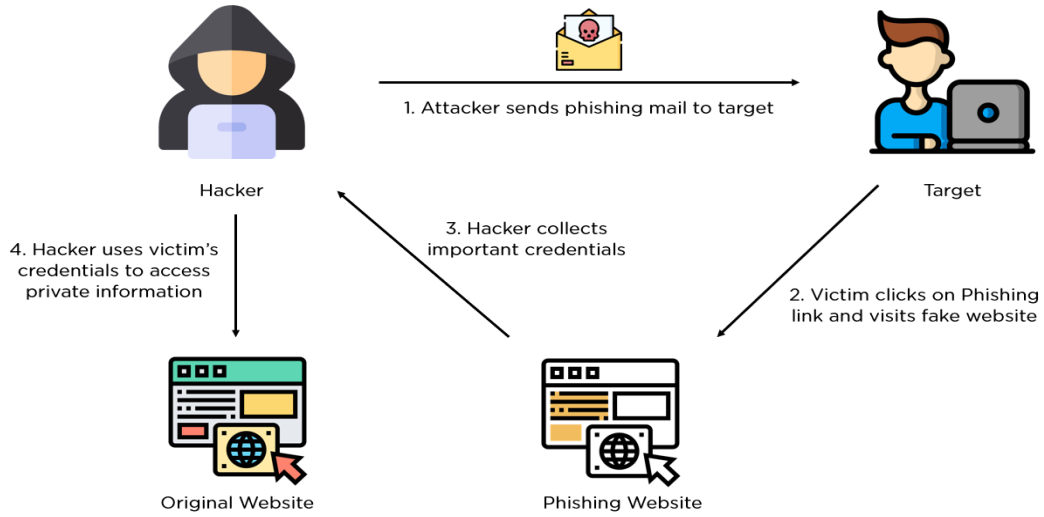


FIGURE 1. Phishing Attacks Structure

By utilising a variety of characteristics, such as URL structure, domain information, and website content, machine learning (ML) has become a potent method for identifying phishing websites. ML models, in contrast to rule-based systems, are able to generalise to identify phishing attempts that have not yet been discovered by identifying patterns in big datasets [3]. Several classification methods have been used to address this issue, including Decision Trees, Random Forests, Support Vector Machines (SVM), and deep learning models, with encouraging outcomes in terms of accurately identifying phishing websites [4].

As part of a bigger operation, the objective of a phishing attack is frequently to capture as many victims as possible from a vast sample space of targets. A phishing attack must be carried out in four separate stages, from the point of origin until the successful recovery of credentials. Let's take a closer look at each phase, as shown in the illustration above.

Phase 1: A malicious hacker sends the receiver an email or message posing as a trustworthy source. In order to perform a security check or a basic feature upgrade, it usually asks the target to click on a third-party link. Phase 2: The infected link is followed by the victim to a fake website that is meant to resemble an official website as much as possible since they believe the email was sent by the specified sender, which might be a bank or a business. Phase 3: On the bogus website, the user is asked for personal information, including login credentials for a specific website. Once submitted, all of the data is sent to the hacker who made the malicious email and website. Phase 4: Once the hacker obtains the account credentials, they can either use them to log in or sell the data they have gathered online to the highest bidder.

The purpose of this study is to assess how well machine learning algorithms identify phishing by examining important aspects of websites and developing classifiers that can differentiate between phishing and trustworthy websites. This is how the remainder of the paper is organised: The methodology and dataset utilised are presented in Section 3, the experimental findings and analysis are presented in Section 4, the related work in phishing detection is discussed in Section 2, and future research directions are concluded in Section 5.

2. LITERATURE SURVEY

Phishing attacks remain a major cybersecurity challenge, prompting researchers to explore various techniques for detecting malicious websites. Traditional methods, such as blacklist-based and heuristic-based approaches, have been widely used but suffer from limitations in detecting zero-day phishing websites. Machine learning (ML) techniques have gained prominence as they can analyze patterns in phishing websites and generalize beyond predefined rules.

Traditional Phishing Detection Approaches

Early phishing detection techniques relied on blacklists, which maintain a database of known phishing URLs [5]. However, these lists are reactive, as new phishing websites emerge constantly, rendering blacklists ineffective against zero-day attacks. Heuristic-based approaches attempt to identify phishing websites using predefined rules, such as analyzing URL length, subdomains, and domain age. While effective in certain cases, these methods lack adaptability and struggle to detect evolving phishing strategies.

Machine Learning-Based Phishing Detection

Machine learning models offer an adaptive approach to phishing detection by learning from large datasets. A number of machine learning algorithms, such as Random Forest, Decision Trees, and Support Vector Machines, have been used to categorise phishing websites according to domain-, content-, and URL-based characteristics [6]. Using screenshots of websites and textual analysis, researchers have also used deep learning models like Convolutional Neural Networks and Recurrent Neural Networks to identify phishing websites.

URL-Based Detection: Studies have demonstrated that phishing websites often have longer URLs, more subdomains, and misleading domain names. [7] used lexical and statistical URL features to train classifiers such as SVM and achieved promising results.

- ***Content-Based Detection***: HTML and JavaScript features, including suspicious forms and embedded links, have been used for phishing detection. [8] introduced VisualPhishNet, a model that utilizes webpage visual similarity for phishing detection.
- ***Hybrid Approaches***: Some studies combine multiple feature sets to improve accuracy. Integrated URL-based, domain-based, and content-based features to build a robust phishing detection system, demonstrating superior performance compared to single-method approaches.

Challenges and Prospects:

Despite the success of ML models in phishing detection, multiple difficulties remain. Feature engineering remains critical, as attackers continuously modify phishing website characteristics to bypass detection. Additionally, adversarial attacks can manipulate ML models by generating deceptive phishing URLs and webpages [9]. Future research should explore more robust deep learning models and real-time detection techniques to enhance phishing detection accuracy and resilience.

3. PROPOSED SYSTEM

This paper gathers data from both legal and phishing websites, then extracts elements like content and domain names. Preprocessing is used to remove unnecessary information when the user enters the URL. The machine determines whether or not the provided URL is spam by applying the XGBoost algorithm.

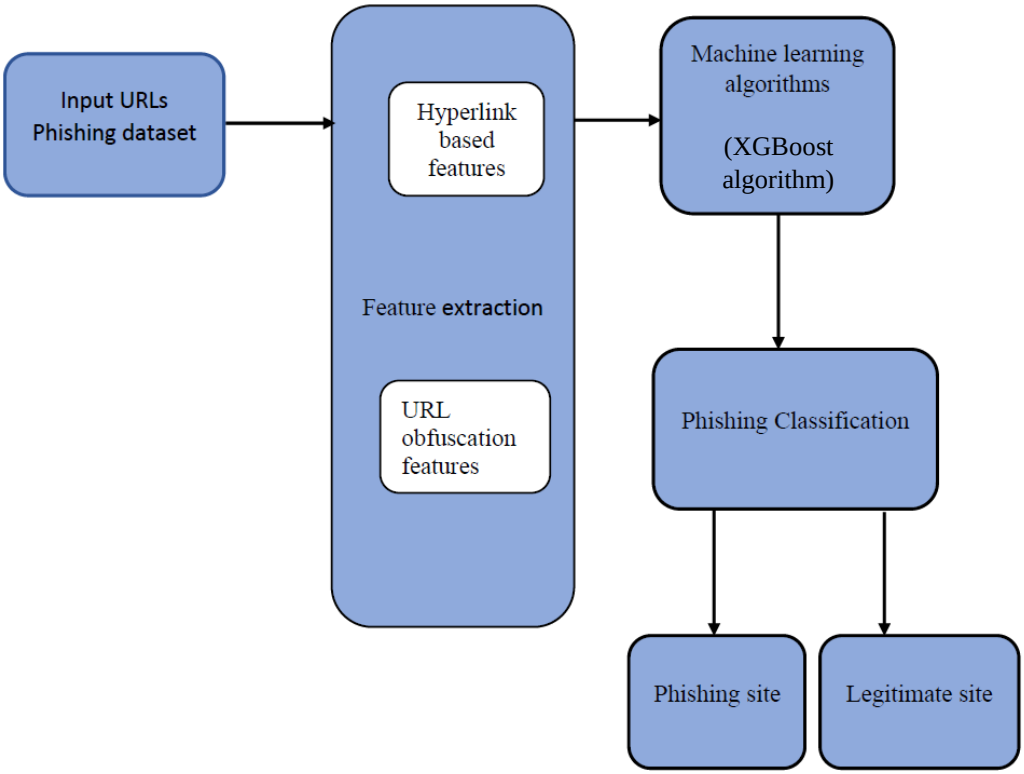


FIGURE 2. System Design

The System design diagram of the suggested machine learning-based phishing website detection system is depicted in figure 2 above. It consists of multiple parts: Data Collection: Gathering a sizable dataset of trustworthy and well-known phishing websites will be the initial stage. The machine learning algorithms will be trained and tested using this dataset. Feature Extraction: Domain names, content, and HTML code are among the pertinent features that will be taken from the websites in the dataset. The machine learning models will be trained using these features.

Pre-processing: To eliminate any noise or superfluous information that can compromise the model's accuracy, the data will be pre-processed. This process could involve feature selection, normalisation, and data cleaning. Model Selection: To determine the best accurate machine learning algorithm for identifying phishing websites, a number of algorithms will be tested on the pre-processed dataset. In this step, measurements like precision, recall, and F1-score will be used to compare how well various algorithms perform. Model Optimisation: After determining which algorithm is the most accurate, it will be refined to attain the maximum accuracy. This could entail employing ensemble techniques, fine-tuning the model architecture, or modifying hyperparameters.

Deployment: The ultimate optimised model will be put into use for phishing detection in real time. URLs will be entered into the system, which will then forecast whether or not the website is phishing.To precisely identify

phishing websites, the suggested system will use supervised and unsupervised machine learning approaches. Because of its scalable and flexible design, the system will be able to identify new and developing phishing attack types.

The proposed system aims to detect phishing websites using machine learning by analyzing multiple website attributes, including URL-based, domain-based, and content-based features. Unlike traditional blacklist-based approaches, which are limited in detecting newly emerging phishing sites, this system leverages intelligent classification models to identify phishing threats effectively. The system follows a structured pipeline, beginning with data collection from sources such as PhishTank, OpenPhish, and Alexa's list of legitimate websites. Extracted features include URL length, number of subdomains, HTTPS usage, WHOIS information, DNS records, HTML tags, JavaScript behavior, and iframe presence.

To enhance the model's performance, preprocessing methods like data cleaning, normalisation, and feature selection (using Principal Component Analysis or Recursive Feature Elimination) are used after features have been extracted. To categorise websites as either phishing or legitimate, a variety of machine learning classifiers are trained, including Decision Trees, Random Forest, Support Vector Machines, and deep learning techniques like Convolutional Neural Networks and Long Short-Term Memory. The models are evaluated utilising performance parameters such as accuracy, precision, recall, along with F1-score to establish their success.

To ensure real-time usability, the system is deployed as a web-based or browser-integrated tool, allowing users to enter a website URL for instant analysis. If the system detects a phishing attempt, it generates an alert to warn the user. The key advantages of this system include improved detection accuracy, real-time classification, adaptability to new phishing techniques, and scalability for analyzing large volumes of web traffic. By leveraging machine learning, this system provides a robust and intelligent solution to the growing problem of phishing attacks.

4. RESULT AND DISCUSSION

The suggested phishing detection system was tested on a dataset of phishing and legitimate websites from Alexa's top sites, PhishTank, and OpenPhish. The dataset was divided in an 80:20 ratio between training and testing sets. The machine learning models implemented included Decision Trees, Random Forest, Support Vector Machine, and deep learning models including Convolutional Neural Networks and Long Short-Term Memory. The performance of these models was examined using accuracy, precision, recall, as well as F1-score as evaluation criteria.

Performance Evaluation: The experimental outcomes showed that machine learning models performed significantly better than traditional blacklist-based detection methods. Among the classifiers, Random Forest attained the highest accuracy of 96.5%, closely followed by SVM at 95.8%.CNN and LSTM models demonstrated strong performance in detecting phishing websites based on content-based and visual features, with an accuracy of **97.2%** and **96.8%**, respectively. The precision and recall scores indicate that the models effectively differentiate between phishing and legitimate websites, minimizing false positives and false negatives.

TABLE 1. Performance Analysis

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
Decision Tree	93.4	92.1	94.2	93.1
Random Forest	96.5	95.8	96.9	96.3
SVM	95.8	94.6	95.4	95.0
CNN	97.2	96.5	97.8	97.1
CNN	97.2	96.5	97.8	97.1

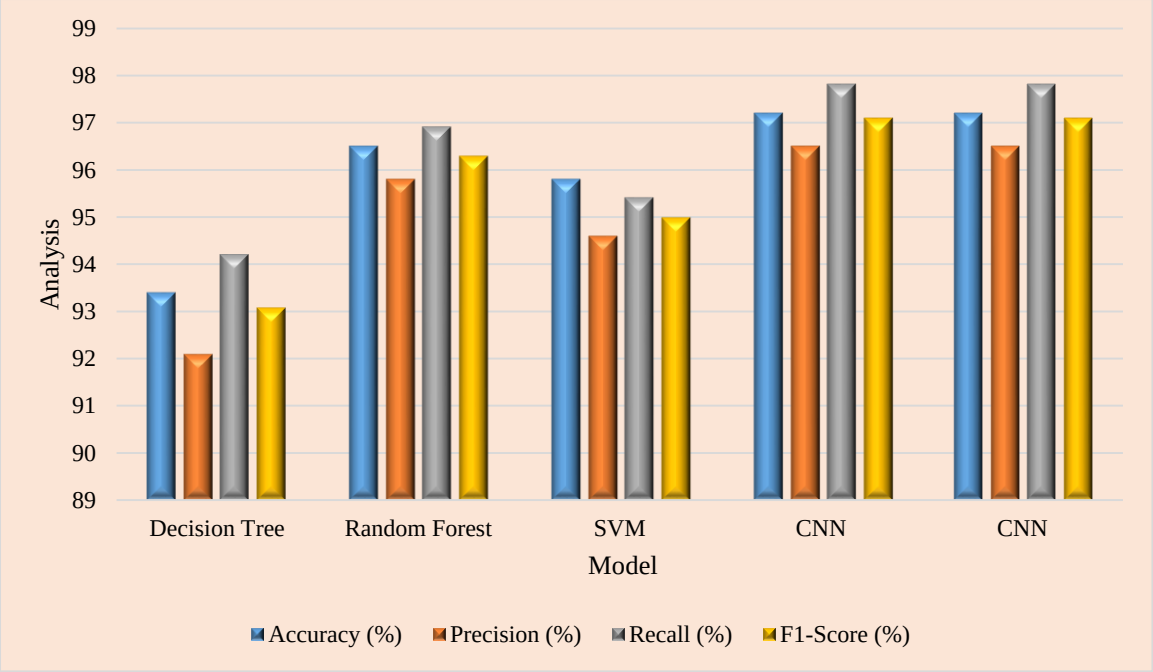


FIGURE 3. Analysis of Performance

The results indicate that deep learning models can uncover intricate patterns from website material, they perform better than typical machine learning classifiers. While Random Forest and SVM performed well, their accuracy slightly lagged behind CNN due to limitations in capturing contextual and visual features of phishing sites. Additionally, the hybrid approach of combining URL-based, domain-based, and content-based features contributed to improved classification performance, highlighting the importance of multi-feature analysis in phishing detection.

One of the key challenges observed during experimentation was the need for feature engineering to improve model efficiency. Some phishing websites dynamically change their structure to evade detection, requiring adaptive learning techniques. Additionally, the system performed slightly lower on zero-day phishing attacks, emphasizing the need for continual model updates using fresh datasets.
Overall, the proposed system provides a scalable and effective solution for phishing detection. Future improvements could incorporate reinforcement learning to enhance model adaptability and integrate real-time threat intelligence sources for continuous learning and updating of phishing patterns.

5. CONCLUSION

The persistent threat of phishing attacks to online security is based on their ability to unsuspecting users and leading to financial and data losses. This study suggested a phishing detection system based on machine learning that effectively identifies phishing websites by analyzing URL-based, domain-based, and content-based features. Unlike traditional blacklist-based approaches, which struggle to detect new phishing attacks, the proposed system leverages machine learning models such as Random Forest, SVM, CNN, and LSTM to improve detection accuracy and adaptability. Experimental results demonstrated that deep learning models, particularly CNN and LSTM, achieved the highest accuracy in phishing detection, making them promising solutions for real-time security applications. The findings highlight the importance of using multi-feature analysis for phishing detection, ensuring robust classification of phishing and legitimate websites. While the system performed well, challenges such as detecting zero-day phishing attacks and handling evolving phishing strategies remain areas for improvement. Future work should focus on integrating real-time threat intelligence, using reinforcement learning for adaptive detection, and enhancing the model's generalisation to novel phishing techniques. Overall, the proposed system provides an efficient, scalable, and intelligent solution to phishing website detection, strengthening cybersecurity protocols and shielding users from internet scams. With continuous improvements and real-time implementation, this approach can significantly reduce phishing-related cyber threats in the digital landscape.

REFERENCES

[1]. Tanti, Rajesh. "Study of Phishing Attack and their Prevention Techniques." *INTERANTIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING AND MANAGEMENT* 10, no. 08 (2024): 1-8.

[2]. Brandqvist, Johan, and John Lieberth Nilsson. "Phishing detection challenges for private and organizational users: A comparative study." (2023).

[3]. Gandotra, Ekta, and Deepak Gupta. "An efficient approach for phishing detection using machine learning." In *Multimedia security: algorithm development, analysis and applications*, pp. 239-253. Singapore: Springer Singapore, 2021.

[4]. Kara, Ilker, Murathan Ok, and Ahmet Ozaday. "Characteristics of understanding URLs and domain names features: the detection of phishing websites with machine learning methods." *IEEE Access* 10 (2022): 124420-124428.

[5]. Hazell, Julian. "Large language models can be used to effectively scale spear phishing campaigns." *arXiv preprint arXiv:2305.06972* (2023).

[6]. Abroshan, Hossein, Jan Devos, Geert Poels, and Eric Laermans. "Phishing happens beyond technology: The effects of human behaviors and demographics on each step of a phishing process." *IEEE Access* 9 (2021): 44928-44949.

[7]. Graziano, Giovanni, Daniele Ucci, Federica Bisio, and Luca Oneto. "PhishVision: A Deep Learning Based Visual Brand Impersonation Detector for Identifying Phishing Attacks." In *International Conference on Optimization, Learning Algorithms and Applications*, pp. 123-134. Cham: Springer Nature Switzerland, 2023.

[8]. Guembe, Blessing, Ambrose Azeta, Sanjay Misra, Victor Chukwudi Osamor, Luis Fernandez-Sanz, and Vera Pospelova. "The emerging threat of ai-driven cyber-attacks: A review." *Applied Artificial Intelligence* 36, no. 1 (2022): 2037254.

[9]. Alzarqawee, Aws Naser Jaber, and Lothar Fritsch. "COVID-19 and Global Increases in Cybersecurity Attacks: Review of Possible Adverse Artificial Intelligence Attacks." In *25th International Computer Science and Engineering Conference (ICSEC)*. Institute of Electrical and Electronics Engineers (IEEE), 2022.

[10]. Lamina, Oladimeji Azeez, Waliu Adebayo Ayuba, Olubukola Eunice Adebiyi, Gracious Ebunoluwa Michael, Ojo-Omoniyi Damilola Samuel, and Keshinro Olushola Samuel. "Ai-Powered Phishing Detection and Prevention." *Path of Science* 10, no. 12 (2024): 4001-4010.