WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Machine Learning Role in Detecting Phishing Websites

Khandavilli Anusha

Student, Rajam, Vizianagaram, 535127, Andhra Pradesh, India.

ABSTRACT

In recent years the usage of multiple services like online banking systems, Education, entertainment, and social networks have accelerated the Web's evolution. It leads to a huge amount of data being downloaded and Transferred to the internet. This allows attackers to access sensitive personal or financial data Such as usernames, passwords, account numbers, and security numbers, this is known as a web phishing attack. So, the users who have updated their details or given credentials to the phishing websites, have been troubled and it leads to financial attacks. This is one of the most Serious issues in web security. This study presents an innovative approach to detecting phishing websites using machine learning techniques, especially using the Multi-Layer Stacked Ensemble Learning Model. By applying these techniques to URL structure to classify the websites into phishing and legitimate. The integration of the Ensemble Learning techniques contributes to a potent solution for identifying fraudulent websites, bolstering online security, and ensuring safer browsing experiences for users. This ensemble model not only enhances accuracy but also demonstrates accuracy robustness in adapting to evolving fake website strategies.

Keywords: *Machine learning, Fake Websites, Phishing Websites, URL, Ensemble learning.*

1. Introduction

Imagine you're on the internet, shopping, emailing, or just browsing for information. It's convenient, right? But there's a hidden danger called phishing. Phishing is when bad actors create fake websites that look real, hoping to trick you into sharing your sensitive information like passwords or credit card numbers. In this term paper, we're going to talk about how computers, specifically through a clever technology called "machine learning," are like digital detectives that help us find and stop these fake websites. Machine learning is like a computer's superpower, where it learns from lots of examples and gets better at recognizing things over time. Our journey begins by understanding how phishing has evolved and how it threatens us online. Then, we'll dive into what machine learning is and how it works, without getting too technical. It's like teaching a computer to spot the difference between real money and counterfeit bills by showing it lots of examples. We'll also explore how machine learning helps us identify fake websites. It's like having a watchdog that can quickly analyse websites and spot suspicious signs that humans might miss. This technology helps keep us safe online. But, it's not all sunshine and rainbows. Machine learning isn't perfect, and we'll talk about its challenges and limitations. We'll also discuss the ethical questions surrounding using these systems to protect us online. In the end, you'll see that machine learning is like a guardian, standing at the gate of our digital world, protecting us from online threats. It's a fascinating partnership between technology and security, making the internet a safer place for everyone. So, let's explore how this digital detective, machine learning, helps keep us safe from phishing websites.

2. Literature Survey

In paper [1]. This paper mentions that there are many anti-phishing techniques, toolbars, extensions, and machine learning algorithms used for the detection of phishing sites. Machine learning-based techniques have played a vital role in the detection of phishing sites, and existing literature shows that they can achieve performance of at least 99%. Some recent and popular anti-phishing techniques mentioned in the literature include the use of machine learning methods such as Logistic Regression, Ada boost, Random Forest, K-Nearest Neighbor, Neural Networks, Support Vector Machine, Gradient boosting, and XGBoost on the UCI phishing dataset. All the above algorithms are integrated together to a multilayer stacked ensemble learning model. So, it has more efficiency because of the structure of the model. Feature selection methods such as Information gain, gain ratio, chi-square, and correlation-based feature selection have also been employed with classification algorithms like Naive-Bayes, K-Nearest Neighbor, Support Vector Machine, Decision Trees, and ID3 on the UCI phishing dataset.

In paper [2]. This paper describes a system that uses a neural network to classify URLs as phishing or non-phishing, with the potential to enhance the accuracy of current phishing detection systems. The authors highlight the importance of detecting and preventing phishing attacks and compare the performance of ML algorithms such as RF, LightGBM, and XGBoost. The RF algorithm achieves the highest accuracy. A systematic literature review of 43 studies identifies that Supervised ML algorithms, particularly Deep Neural Networks, are prevalent in phishing detection. DL algorithms have the potential to strengthen online system security. Another study focuses on detecting phishing websites using ML techniques and Convolutional Neural Networks (CNN). The study compares the accuracy of SVM, RF, and CNN algorithms, with CNN achieving the highest accuracy.

In paper [3]. This paper discusses the evolving nature of phishing attacks and the need for novel and efficient countermeasures in the field of cybersecurity. Artificial Intelligence (AI) schemes have been widely used for mitigating phishing attacks, but they have their shortcomings, such as high false alarm rates and the inability to interpret phishing methods. The paper proposes four meta-learner models developed using the extra-tree base classifier for detecting phishing websites. These models achieved a detection accuracy of at least 97% with a low false-positive rate. The proposed models outperform existing machine learning-based models in phishing attack detection. The adoption of meta-learners is recommended for building phishing attack detection models.

In paper [4]. Machine learning can detect phishing websites by classifying and labeling the URLs and domain names of websites based on identified features. They separately used some machine learning algorithms like SVM, naïve bayes etc. with 83 % and 92% respectively.

The proposed method in the current paper goes beyond analyzing HTML, DOM, and URL-based features by considering URLs and domain names. It achieves a 98.90% accuracy in detecting phishing websites using six different classifier algorithms, with Random Forest algorithm showing the highest accuracy rate.

In paper [5]. This paper proposes a boosting-based hybrid feature selection and multi-layer stacked ensemble learning model for detecting phishing websites. The authors mention that phishing attacks are a common threat and have been around for a long time. The proposed model achieved an accuracy ranging from 96.16% to 98.95% without feature selection and from 96.18% to 98.80% with feature selection, outperforming existing models. This paper also mentions different categories of feature selection techniques, including filter, wrapper, embedded, hybrid, and others.

3. Methodology

Here's a methodology flow for Machine Learning Role in Detecting Phishing:

1. Data Collection and Preprocessing:

- Gather a dataset containing features that distinguish phishing websites from legitimate ones. These features often include:
    - URL-based features (length, presence of special characters, domain age)
    - Domain-based features (IP address, WHOIS information)
- Preprocess the data:
    - Handle missing values and outliers.
    - Normalize or standardize features if necessary.
    - Split the data into training and testing sets.

1. Layered Ensemble Construction:

- Create multiple layers of base learners:
    - Employ diverse classifiers like decision trees, support vector machines, random forests, logistic regression, and others.
    - Each layer trains independently on the original dataset.
- Stack the layers:
    - The predictions from each layer become inputs for the next layer.
    - The final layer is a meta-learner that combines the predictions of all base learners. Mono conversion: Transform stereo tracks to mono if necessary.

3. Model Training:

- Train each base learner:
    - Optimize hyperparameters for each classifier within each layer.
- Train the meta-learner:
    - Utilize another supervised learning algorithm (e.g., logistic regression, decision tree) to learn how to combine predictions from the base learners effectively. Spectral density

4. Model Evaluation:

- Assess the model's performance on the testing dataset using metrics like:
    - Accuracy

- Precision
- Recall
- F1-score
- AUC-ROC curve

- Compare with other standalone classifiers and ensemble techniques.

5. Model Deployment:

- Integrate the model into a phishing detection system to classify new websites as legitimate or phishing in real-time.

Additional considerations:

- Feature Selection: Identify the most relevant features to improve model performance and reduce computational cost.
- Hyperparameter Tuning: Optimize hyperparameters for both base learners and the meta-learner.
- Cross-Validation: Employ cross-validation techniques to prevent overfitting and assess model generalization.
- Online Learning: Consider updating the model with new data to adapt to evolving phishing techniques.

4. Results and Discussion

The paper introduces the innovative concept of Multilayer Stacked Ensemble Learning and applies a repertoire of traditional learning techniques across four diverse datasets. Notably, the performance of well-established algorithms like XGBoost (XGB) and Random Forest (RF) exceeded other contenders but fell short of the benchmark set by MLSELM. Thus, there is a discernible call to augment the integration of XGB and RF algorithms within the MLSELM framework. The assessment of model performance is conducted using crucial classification metrics—precision, recall, F-score, and accuracy. In the nuanced context of distinguishing between Legitimate and Phishing elements, instances of phishing are aptly designated as positive, establishing a clear contrast with the negative categorization for legitimate occurrences. MLSELM shines in performance when implementing data balancing techniques, showcasing superiority in scenarios where imbalanced data pose a challenge. The proposed methodology employs data balancing through Random Under Sampling and Random Over Sampling, strategically addressing the intricacies of class imbalance. To further enhance data balancing, the paper advocates for the integration of deep learning techniques as an alternative to conventional methods such as random under-sampling and random over-sampling. Techniques like generative adversarial networks (GANs) and autoencoders emerge as potent tools for generating synthetic samples for the minority class, effectively mitigating the challenges associated with class imbalance. However, the comprehensive effectiveness of MLSELM is tempered by a recognized limitation—the heightened computational overhead arising from the intricate stacking of classifiers at multiple layers. In response, the paper proposes a suite of strategic measures including model pruning, judicious optimization algorithm selection, parallelization for efficient computation, feature reduction, selective stacking, ensemble learning, harnessing hardware acceleration, thoughtful optimal layer design, and the adoption of incremental learning techniques. The paper underscores the importance of systematic experimentation with these strategies to strike a delicate balance between model complexity and computational efficiency, a balance tailored to the unique characteristics of the dataset at hand and the available computational resources.

5. Conclusion

The paper introduces an innovative multilayer stacked ensemble learning model designed specifically for the detection of phishing websites, representing a significant advancement in the field. The model's effectiveness is underscored by its consistently high accuracy, ranging impressively from 96.79% to 98.90%, as demonstrated across various datasets during rigorous evaluations. In contrast to baseline models, the proposed multilayer stacked ensemble learning model not only showcased superior accuracy but also excelled in terms of F-score metrics. This indicates not only a general precision in classification but also a robust performance in capturing the balance between precision and recall, marking a notable improvement over conventional approach. A notable observation from the evaluation is the enhanced performance of the MLSELM model when confronted with balanced data compared to scenarios involving imbalanced data. This insight sheds light on the model's sensitivity to class distribution, emphasizing the importance of addressing data imbalance for optimal results. To further elevate the model's capabilities, the authors are strategically planning to delve into feature selection algorithms. This includes an exploration of various techniques for selecting the most informative features, a critical step in refining the model's focus on relevant aspects of the data. Additionally, the authors aim to synergize feature selection algorithms with tuning parameters, a synergistic approach that holds promise for fine-tuning the model's performance and adaptability. In summary, the paper not only introduces a powerful multilayer stacked ensemble learning model for phishing detection but also provides empirical evidence of its effectiveness through comprehensive evaluations. The ongoing commitment to refining the model, incorporating feature selection algorithms, and leveraging tuning parameters positions this research on the cutting edge of advancements in the field of cybersecurity.

REFERENCES

[1] L. R. Kalabarige, R. S. Rao, A. Abraham and L. A. Gabralla, "Multilayer Stacked Ensemble Learning Model to Detect Phishing Websites," in IEEE Access, vol. 10, pp. 79543-79552, (2022).

[2] Sajadul Islam, Nusrat Jahan Jyoti, Solaiman Mia, Gulzar Hussain, 'Fake Website Detection Using Machine Learning Algorithms', June 2023.

[3] Yazan Ahmad Alsariera 1, Victor Elijah Adeyemo 2, Abdullateef Oluwagbemiga Balogun 3, And Ammar Kareem Alazzawi3, 'AI Meta-Learners and Extra-Trees Algorithm forthe Detection of Phishing Websites', August 2023.

[4] Ilker Kara 1, Murathan Ok 2, And Ahmet Ozaday2, 'Characteristics of Understanding URLs and Domain Names Features: The Detection of Phishing Websites with Machine Learning Methods', November 2022.

[5] Lakshmana Rao Kalabarige1, Routhu Srinivasa Rao 2, Alwyn R. Pais3, And Lubna Abdelkareim Gabralla4, 'A Boosting-Based Hybrid Feature Selection and Multi-Layer Stacked Ensemble Learning Model to Detect Phishing Websites', July 2023.