International Journal of Advanced Trends in Engineering and Management
(ISSN 2583-7052)

pp. 15-17, May

PHISHNET: Threat Intelligence System for Phishing Attacks Using Machine Learning

A Mahesh[1*], Bale Mounika[2], Sneha L[3], Varsha L[4], Bhavya M[5]

[1]Professor Department of Computer science and Engineering, Sri Sairam College of Engineering, Bangalore-560126.
[2,3,4,5] Final Year of Computer science and Engineering, Sri Sairam College of Engineering, Bangalore-560126.

ABSTRACT: Phishing attacks remain a significant threat to cybersecurity, targeting individuals and organizations alike. This paper introduces PHISHNET, a comprehensive threat intelligence system that leverages machine learning techniques to detect and mitigate phishing attacks across three communication vectors: URLs, emails, and SMS messages. The system employs Gradient Boosting for URL detection, achieving an accuracy of 98%, while Random Forest algorithms are utilized for email and SMS detection, attaining accuracies of 97% and 96%, respectively. By analyzing various features related to URLs and extracting content from emails and SMS messages, PHISHNET provides users with actionable insights to enhance their security posture against phishing threats.

Keywords: Feature Extraction, URL Analysis, Real-Time Detection, Cybersecurity, Building Classification, Machine Learning

1. Introduction

Phishing attacks have become a major online threat, using tricks to steal personal information like passwords and credit card details. Since traditional security methods often fail to keep up with these evolving threats, machine learning is now being used to detect phishing more effectively. This paper introduces PHISHNET, a system that uses machine learning to spot phishing in URLs, emails, and SMS messages. It uses Gradient Boosting to check URLs and Random Forest models to analyze message content. PHISHNET also personalizes its detection by considering user preferences and demographics, which helps build trust and improve accuracy. It tackles the challenge of new users (the cold start problem) and stays up-to-date by adjusting to changes in phishing tactics over time. Overall, PHISHNET offers a smart, adaptive way to fight phishing using advanced technology.

2. Recent Works

Several studies in recent years have focused on improving phishing detection using machine learning techniques. Adarsh Mandadi et al. (2022) examined various machine learning models for phishing website detection, highlighting the importance of optimized feature selection for better accuracy. Edward Wijaya et al. (2023) proposed a hybrid model combining Naïve Bayes, SVM, LSTM, and CNN for SMS spam detection, emphasizing model robustness and adaptability. Ammar Odeh et al. (2021) reviewed different machine learning approaches for phishing detection and stressed the benefits of combining algorithms to address evolving threats. V. Dharani et al. (2023) focused on detecting phishing in SMS and email using machine learning classifiers, underlining the role of effective feature extraction and training. Kerin Pithawala et al. (2021) explored classification techniques for phishing URL detection based on URL characteristics. While these studies demonstrate significant

advancements, many rely heavily on static datasets or lack personalization features. In contrast, our PHISHNET system not only integrates multiple machine learning models for URLs, emails, and SMS detection but also incorporates user behavior, demographic data, and temporal factors to deliver adaptive, personalized, and up-to-date threat detection without depending solely on static datasets.

3. Proposed Work Explanation

In the evaluation phase, the performance of each PHISHNET model is assessed by inputting the prepared test datasets into their respective trained models—URL Detection, Email Detection, and SMS Detection. Each model predicts whether the input is phishing or legitimate, and these predictions are then compared with the actual labels from the dataset. This comparison helps determine the accuracy and effectiveness of each model in correctly identifying phishing attempts. The overall evaluation provides insight into how well PHISHNET performs in real-world scenarios by measuring prediction accuracy and reliability.

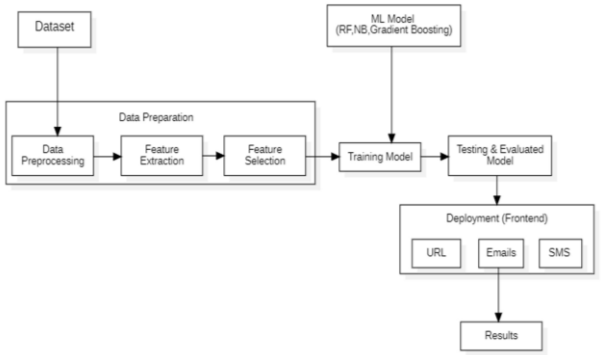

Figure 1: *Architecture Diagram*

Figure 2: *Learning Model from Proposed System*

4. Results and Discussion

To validate the machine learning models developed for phishing detection in our project, we utilized accuracy as the primary metric for evaluation. Accuracy is a widely recognized measure in classification tasks due to its simplicity and ease of interpretation. It provides a clear indication of a model's performance by calculating the proportion of correct predictions made by the model. The formula for accuracy can be expressed as follows:

$$Accuracy = \frac{Numberofcorrectpredictions}{Totalnumberofpredictions} \quad (1)$$

In a more detailed context, accuracy can also be calculated using the following equation:

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \quad (2)$$

Where:

- TP*TP* represents True Positives,
- FP*FP* denotes False Positives,
- TN*TN* stands for True Negatives,
- FN*FN* indicates False Negatives.

In this project, we trained models for three distinct types of phishing detection: URLs, emails, and SMS messages. Each model was evaluated based on its ability to accurately classify instances as phishing or legitimate. The experimental evaluation yielded the following results:

1. **URL Detection Model**: Implementing Gradient Boosting algorithms, this model achieved an impressive accuracy of **98%** in identifying phishing URLs.
2. **Email Detection Model**: Utilizing Random Forest algorithms, this model successfully classified emails with an accuracy of **97%**, effectively distinguishing between spam and legitimate messages.
3. **SMS Detection Model**: Also based on Random Forest algorithms, this model

reached an accuracy of 96% in detecting spam SMS messages.

These results demonstrate the effectiveness of the selected algorithms in accurately identifying phishing threats across different communication channels, highlighting the robustness of our approach in combating phishing attacks.

5. Conclusion

In this project, we built and tested machine learning models to detect phishing threats through URLs, emails, and SMS messages. Our models performed well, with 98% accuracy for URLs using Gradient Boosting, and 97% and 96% accuracy for emails and SMS using Random Forest. These results show that machine learning is a powerful tool for spotting phishing attacks and improving online security. The success of these models suggests they can help organizations protect users more effectively. For future improvements, we plan to use larger and more diverse datasets to make the models even more reliable. Adding features like user behavior analysis and combining different algorithms (ensemble methods) could boost performance. We also aim to create real-time detection systems for faster responses and explore ways to protect our models from advanced attacks through adversarial machine learning. Overall, our goal is to keep improving the system to stay ahead of evolving phishing threats and create a safer digital space.

References

1. Adarsh Mandadi; Saikiran Bopanna; Vishnu Ravella; R. Kavitha, Year: 2022, “Phishing website detection Using Machine Learning”, 2022 IEEE 7th International Conference for Convergence in Technology (I2CT), pp. 1 – 4.

2. Edward Wijaya; Gracella Noveliora; Kharisma Dwi Utami; Rojali; Ghinaa Zain Nabiilah, Year: 2023, “Spam Detection in Short Message Service (SMS) Using Naïve Bayes, SVM, LSTM, and CNN”, 2023 10th International Conference on Information Technology, Computer and Electrical Engineering (ICITACEE), pp. 431 – 436.

3. Ammar Odeh; Ismail Keshta; Eman Abdelfattah, Year: 2021, “Machine Learning Techniques for detection of Website Phishing: A Review for Promises and Challenges”, 2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC).

4. V Dharani; Divyashree Hegde; Mohana, Year: 2023, “Spam SMS (or) Email Detection and Classification using Machine Learning”, 2023 5th International Conference on Smart Systems and Inventive Technology (ICSSIT), pp. 1104 –1108.

5. Kerin Pithawala; Sakshi Jagtap; Preksha Cholachgud, Year: 2021, “Detecting Phishing of Short Uniform Resource Locators using classification techniques, 2021 12th International Conference on Computing Communication and Networking Technologies (ICCCNT), pp. 1 – 5.