2023 Congress in Computer Science, Computer Engineering, & Applied Computing (CSCE) | 979-8-3503-2759-5/23/$31.00 ©2023 IEEE | DOI: 10.1109/CSCE60160.2023.00371

PhishGuard: Machine Learning-Powered Phishing URL Detection

Saydul Akbar Murad[1], Nick Rahimi[1]*, and Abu Jafar Md Muzahid[2]
[1]*School of Computing Sciences & Computer Engineering, University of Southern Mississippi, Hattiesburg, USA*
[2]*Faculty of Computing, University Malaysia Pahang, Pahang, Malaysia*
E-mail: saydulakbar.murad@usm.edu, nick.rahimi@usm.edu, mrumi98@gmail.com

***Abstract*—Phishing is a major threat to internet security, targeting human vulnerabilities instead of software vulnerabilities. It involves directing users to malicious websites where their sensitive information can be stolen. Many researchers have worked on detecting phishing URLs, but their models have limitations such as low accuracy and high false positives. To address these issues, we propose a machine-learning model to detect phishing URLs. To detect these malicious URLs, we use a dataset of over 500K entries collected from the Kaggle website. The dataset is used to train five supervised machine-learning techniques, including K-Nearest Neighbors (KNN), Logistic Regression (LR), Decision Tree (DT), Support Vector Machine (SVM), and Random Forest (RF). The aim is to improve the performance of the classifier by studying the features of phishing websites and selecting a better combination of them. To measure the performance, we considered three parameters: accuracy, precision, and recall. The LR technique yielded the best performance, demonstrating its efficacy in detecting phishing URLs.**

***Index Terms*—Phishing URL, Machine Learning, KNN, SVM, Logistic Regression.**

I. Introduction

Phishing is a form of online deception where fraudsters fabricate fraudulent websites or emails that seem genuine to dupe users into divulging sensitive information, such as credit card details or login credentials [1]. In recent times, phishing has emerged as one of the most prominent cybersecurity menaces. Phishing attacks can be very effective because they exploit human vulnerabilities rather than technical vulnerabilities. These attacks often use social engineering techniques to trick users into giving away sensitive information, such as login credentials and personal information. Phishing URL detection refers to the process of identifying and blocking URLs (Uniform Resource Locators) that lead to phishing websites [2]. This involves using various techniques to analyze URLs and their associated web content to determine whether they are legitimate or malicious.

As a result, many organizations and individuals have become more aware of the dangers of phishing and have taken steps to protect themselves. One of the most effective ways to prevent phishing attacks is to detect and block phishing URLs. Phishing URL detection research has been ongoing for several years, and it has become increasingly important as phishing attacks have become more sophisticated. Researchers have developed various techniques and algorithms to identify phishing URLs based on different characteristics, such as the URL structure, domain reputation, and content analysis. Some common techniques used in phishing URL detection include:

- **Blacklisting:** This involves maintaining a list of known phishing URLs and blocking access to them.
- **Machine learning:** This involves training models to identify patterns in phishing URLs and using those models to detect new phishing URLs.
- **URL analysis:** This involves analyzing the structure and content of URLs to identify suspicious or malicious characteristics.
- **Domain reputation analysis:** This involves analyzing the reputation of the domain associated with a URL to determine whether it is likely to be malicious.
- **Content-based analysis:** This involves analyzing the content of a webpage associated with a URL to determine whether it is likely to be malicious.

All the techniques mentioned for detecting phishing websites have their limitations. For instance, the blacklist technique relies on an up-to-date and comprehensive list of known malicious URLs or IP addresses, but attackers can easily create new phishing websites or move their operations to new IP addresses, making it difficult to maintain an accurate blacklist. URL analysis may not be effective at detecting phishing attacks that use legitimate websites as a platform. For example, an attacker may create a phishing email that links to a legitimate website but directs the user to enter sensitive information on a fake login page. In this case, the URL analysis may not detect any malicious activity, as the website itself is legitimate. The drawback of domain reputation analysis is that it focuses on the domain name itself, rather than the content of the website. This means that even if a domain has a good reputation, it may still be hosting phishing content or other malicious activity. In Content-based analysis, attackers can use techniques such as URL cloaking or obfuscation to hide the true destination of a link or to make the phishing content appear legitimate. This can make it difficult for content-based analysis to detect phishing websites.

To overcome those limitations, machine learning and deep learning techniques have been widely used for phishing URL detection, allowing for the creation of more accurate models that can detect even previously unseen phishing URLs. In [3], Zamir, Ammara, et al. introduced a framework for identifying

979-8-3503-2759-5/23/$31.00 ©2023 IEEE
DOI 10.1109/CSCE60160.2023.00371