**ABSTRACT**

Chrome Extension for Detecting Phishing Websites

The proliferation of phishing attacks poses a significant threat to online security, leading to financial losses and compromised personal information. Detecting phishing websites in real-time is crucial to safeguard users from these malicious activities. This project presents a novel approach to identifying phishing websites using a Chrome extension, designed to analyze various features of URLs and web page elements.

Our method employs a feature-based analysis to evaluate the legitimacy of a website. The extension examines multiple characteristics, such as the presence of IP addresses in URLs, the length of URLs, the use of alphanumeric characters, and the presence of special characters like hyphens. For instance, URLs containing IP addresses or excessive length can be indicative of phishing attempts, as legitimate websites typically use domain names and have concise URLs. The extension also evaluates the presence of suspicious characters and patterns in URLs, such as hyphens and multiple subdomains, which are often used to deceive users.

Additional checks include the examination of domain irregularities, favicon consistency, HTTPS usage, and the sourcing of images and scripts from different domains. Favicon consistency is assessed by comparing the domain of the favicon URL with the main domain, as discrepancies can suggest a phishing attempt. Similarly, the extension analyzes the use of HTTPS, as the presence of HTTPS does not necessarily guarantee security but its absence can be a red flag. The extension also scrutinizes the sources of images and scripts; a high percentage of these elements sourced from different domains may indicate a phishing site.

To enhance the accuracy of detection, we integrated several machine learning models, including Neural Networks, Random Forests, and Support Vector Machines (SVM). These models are trained on a labeled dataset of URLs, learning to differentiate between phishing and legitimate websites based on their features. The dataset comprises a diverse range of examples to ensure the models are robust and can generalize well to new, unseen websites. The training process involves feature extraction from URLs and web page elements, followed by model training and validation to optimize performance.

By leveraging a weighted prediction model, the extension aggregates these features to classify websites as either phishing or legitimate. The expected outcome is an effective real-time warning system that alerts users when a potential phishing attempt is detected, thereby enhancing their online security. This project not only provides a practical tool for end-users but also contributes to the broader efforts in combating cybercrime by reducing the incidence of successful phishing attacks. The development and deployment of this Chrome extension represent a significant step towards making the internet a safer place for all users.